newwave

Provider Management System

AHCCCS/Med-QUEST

Arizona Health Care Cost Containment System

Volume I – Technical Proposal

March 15, 2018 **Solicitation # YH18-0033**

Submitted by:
NewWave Telecom & Technologies, Inc.
6518 Meadowridge Road, Ste. 100 • Elkridge, MD 21075
Patrick Munis, President & CEO 410-740-0035 • patrick.munis@newwave.io

Submitted to:
Alice McLain, Procurement Officer
AHCCCS • 701 E. Jefferson, MD5700 • Phoenix, Arizona 85034
602-417-5957 • procurement@azahcccs.gov

newwave.io

This proposal includes data that shall not be disclosed outside the Government and shall not be duplicated, used or disclosed in whole or in part for any purpose other than to evaluate this proposal. If, however, a contract is awarded to this offeror as a result of, or in connection with this submission of this data, the Government shall have the right to duplicate, use or disclose the data to the extent provided in the resulting contract. This restriction does not limit the Government to use information contained in this data if it is obtained from another source without restriction.

OFFEROR'S CHECKLIST (ATTACHMENT D)
Solicitation #YH18-0033

Provider Management System

AHCCCS/Med-QUEST

Arizona Health Care Cost Containment System

Volume I – Technical Proposal

March 15, 2018 **Solicitation # YH18-0033**

Submitted by:
NewWave Telecom & Technologies, Inc.
6518 Meadowridge Road, Ste. 100 • Elkridge, MD 21075
Patrick Munis, President & CEO 410-740-0035 • patrick.munis@newwave.io

Submitted to:
Alice McLain, Procurement Officer
AHCCCS • 701 E. Jefferson, MD5700 • Phoenix, Arizona 85034
602-417-5957 • procurement@azahcccs.gov

This proposal includes data that shall not be disclosed outside the Government and shall not be duplicated, used or disclosed in whole or in part for any purpose other than to evaluate this proposal. If, however, a contract is awarded to this offeror as a result of, or in connection with this submission of this data, the Government shall have the right to duplicate, use or disclose the data to the extent provided in the resulting contract. This restriction does not limit the Government to use information contained in this data if it is obtained from another source without restriction.

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

#	SUBMISSION REQUIREMENTS	OFFEROR'S PROPOSAL PAGE #	OFFEROR'S VOLUME
1	One (1) Hard Copy Proposal, 1 Electronic Copy	n/a	Volume I & Volume II
2	Submittal Cover Letter	v-vi	Volume I
3	Offeror's Checklist (see ATTACHMENT D - this page)	i	Volume I & Volume II
4	Completed and Signed Offer and Acceptance page	Page 163	Volume I
5	Signed Solicitation Amendments, if any (signature page only)	n/a	Volume II
6	Method of Approach - Written narrative in response to requirements with reference to requirement paragraph number.	Page 1-54 (Gantt pgs 30-34)	Volume I
7	Experience and Expertise of the Firm and Key Personnel – Written Narrative • Successful and reliable experience in related past performance • Detailed related information and resumes of Key Personnel • Organizational Chart	Page 55-75 Page 55 Page 74 and Appendix D Page 75	Volume I
8	A completed Arizona Baseline Infrastructure Security Controls 2017 (see Attachment A).	n/a	Thumb Drive for Vol II only
9	Pricing Schedule (see ATTACHMENT B)	n/a	Volume II
10	Certification of Boycott of Israel (see ATTACHMENT C)	n/a	Volume II
11	Statement of Intent to provide Certificate of Insurance	n/a	Volume II
12	Detailed Legal Analysis (If any portions are requested to be kept confidential or proprietary) If any pieces of your proposal are **being requested to be kept confidential, and withheld from public viewing**, please submit an additional redacted copy of the proposal ON A SEPARATE CD. Our office does not require a hard copy of the redacted proposal, only an electronic copy. This will ensure that our office is crystal clear on which version of your proposal is acceptable for public viewing.	n/a	N/A
	Demo here with		

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

TABLE OF CONTENTS

Submittal Cover Letter vi

Tab A. Proposed Method of Approach 1
A.1 Overall Requirements (SOW 5.1) 2
A.2 Documentation and Certification (SOW 5.2) 6
A.3 Regulatory System Compliance (SOW 5.3) 6
A.4 System Architecture (SOW 5.4) 8
A.5 Determine Provider Eligibility (SOW 5.5) 11
A.6 Enroll Provider (SOW 5.6) 14
A.7 Disenroll Provider (SOW 5.7) 14
A.8 Inquire Provider Information (SOW 5.8) 14
A.9 Manage Provider Information (SOW 5.9) 15
A.10 Manage Provider Communication (SOW 5.10) 16
A.11 Perform Provider Outreach (SOW 5.11) 16
A.12 Manage Provider Grievance (SOW 5.12) 17
A.13 Reporting (SOW 5.13) 17
A.14 Solution Help System (SOW 5.14) 19
A.15 System Availability (SOW 5.15) 20
A.16 Security (SOW 5.16) 21
A.17 Project Governance (SOW 5.17) 24
A.18 Project Management (SOW 5.18) 24
A.18.a Project Management Plan 29
A.18.b Project Work Plan (Gantt Chart) 29
A.19 Training (SOW 5.19) 34
A.20 Testing (SOW 5.20) 35
A.21 Maintenance/ Operations (SOW 5.21) 37
A.22 Business Process Redesign 39
A.23 Requirements Confirmation 40
A.24 Software Configuration 40
A.25 Software Development (if applicable) 42
A.26 Security Configuration 42
A.27 Documentation 60
A.28 Knowledge Transfer 63
A.29 Cultural Change Management and Communication 64
A.30 Deployment and Roll Out Support 65
A.31 Production Transfer 67
A.32 Post-Implementation Support 67

Tab B: Experience and Expertise of the Firm and Key Personnel ..... Error! Bookmark not defined.
B.1 Past Performance (SOW 3.2.1) ..... Error! Bookmark not defined.

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

B.1.a NewWave's Experience ..... Error! Bookmark not defined.
Chronic Condition Warehouse (CCW) and Virtual Research Data Center (VRDC) Error! Bookmark not defined.
Enterprise Privacy Policy Engine (EPPE) ..... Error! Bookmark not defined.
Risk Adjustment Data Validation (RAD-V) Clinical Data Abstraction Tool (CDAT) Error! Bookmark not defined.
Medicaid and Children's Health Insurance Program Business Information Systems (MACBIS) System Integrator ..... Error! Bookmark not defined.
Transformed Medicaid Statistical Information System (T-MSIS) Error! Bookmark not defined.
B.1.b IBM Watson Health's Experience ..... Error! Bookmark not defined.
The State of Minnesota, Department of Human Services ..... Error! Bookmark not defined.
North Carolina Department of Health and Human Services ..... Error! Bookmark not defined.
The County of San Diego Health and Human Services Agency. Error! Bookmark not defined.
B.2 Personnel ..... Error! Bookmark not defined.
B.2.a Organizational Chart ..... Error! Bookmark not defined.
Appendix A: Cúram Screen Shots 70
Appendix B: Project Management Plan 86
Appendix C: Project Work Plan Task List 122
Appendix D: Resumes ..... Error! Bookmark not defined.
Appendix E: Completed and Signed Offer and Acceptance ..... Error! Bookmark not defined.
Appendix F: List of Acronyms 154

PAGE COUNT MATRIX

Technical Proposal Section	Page Numbers	Within Page Limit
Submission Cover Letter	v-vi	N/A
Tab A: Proposed Method of Approach	Pages 1-29, 35-54	Yes (within 50 pages)
Gantt Chart Timeline	Pages 30-34	Yes (within 5 pages)
Tab B: Experience and Expertise of the Firm and Key Personnel	Pages 55-75	N/A
Organizational Chart	Page 75	N/A
Appendix A: Cúram Screen Shots	Pages 76-88	N/A
Appendix B: Project Management Plan	Pages 89-121	N/A
Appendix C: Project Work Plan Task Lists	Pages 122-126	N/A
Appendix D: Resumes	Pages 127-162	N/A
Appendix E: Completed and Signed Offer and Acceptance	Page 163	N/A
Appendix F: List of Acronyms	Pages 164-169	N/A

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

LIST OF FIGURES

Figure 1: Team NewWave's Provider Management Solution 2
Figure 2: Reporting Process 17
Figure 3: Team NewWave's PMO Approach 25
Figure 4: Agile Implementation Approach ..... Error! Bookmark not defined.
Figure 5: Gantt Chart for Provider Management System Implementation 33
Figure 6: Continuous Integration and Continuous Delivery (CI/CD) Pipeline Process Overview 41
Figure 7: Network Security Architecture 43
Figure 8: PMS System Security Tools 44
Figure 9: New Relic Portal Screen Shot 59
Figure 10: MECL Module Certification Steps 63
Figure 11: Team NewWave's Organizational Chart ..... Error! Bookmark not defined.
Figure 12: Guided Process for Provider Enrollment 71
Figure 13: Provider Home Page 72
Figure 14: Provider Enrollment – required documentation 74
Figure 15: Enrollment Specialist Dashboard 75
Figure 16: Provider Portal Home Page 76
Figure 17: Application Evidence Dashboard 77
Figure 18: Application Verifications 78
Figure 19: Application ACA Screening 79
Figure 20: Provider Site Visits 80
Figure 21: Provider Notification 81
Figure 22: Provider Types 82
Figure 23: Application Home Page 85

LIST OF TABLES

Table 1: Tools and Processes Used for Tracking Project Action Items ..... Error! Bookmark not defined.

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

SUBMITTAL COVER LETTER

NewWave Telecom & Technologies, Inc.
6518 Meadowridge Road, Suite 100
Elkridge, MD 21075
Phone: 410-782-0476
Fax: 410-379-8338
March 15, 2018

Ms. Alice McLain
Procurement Manager
Arizona Health Care Cost Containment System
701 E. Jefferson, MD5700
Phoenix, AZ 85034

Re: Provider Management System, Solicitation #YH18-0033

Enclosures:

- Volume I—Technical Proposal

Dear Ms. McLain,

NewWave Telecom & Technologies, Inc. (NewWave) and our subcontractor, IBM Watson Health, are pleased to submit this proposal to the Arizona Health Care Cost Containment System (AHCCCS) for the Provider Management System, Solicitation YH18-0033.

As requested, we are submitting our response via hard copy as well as electronic format. NewWave agrees with all terms, conditions, and provisions included in the solicitation and will furnish any or all items on which prices are offered at the price set opposite each item. Our submission is valid for 120 days from the date of submission (March 15, 2018).

We have assembled a team for this opportunity that consists of NewWave and IBM Watson Health—each brings specific strengths and experience to create a comprehensive commercial off-the-shelf (COTS) Provider Management System to both Arizona and Hawaii.

Why Team NewWave? NewWave and IBM Watson Health have a history of working together to solve challenging issues, including most recently at CMS, where we worked with IBM Watson Health to reduce service desk costs related to the rollout of the Quality Payment Program (QPP).

We look forward to working with AHCCCS/Med-QUEST on this important effort. If you have any questions regarding our submission, please email patrick.munis@newwave.io or, if you need to speak with someone directly, contact Ms. Cecilia Bell, NewWave's Director of Contracts, at 410-782-0476, extension 2005.

Changes to document here for demo.

Sincerely,

Patrick Munis

Patrick Munis
President, CEO

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

Throughout our extensive, 13-year history supporting and advising the Centers for Medicare and Medicaid Services (CMS) on its technological efforts, NewWave has remained progressive, combining innovation with institutional knowledge across many Medicare and Medicaid programs. With $300 million in federal government contracts (across eight prime contracts), NewWave plays an integral role in supporting provider programs and national Medicare and Medicaid healthcare programs.

NewWave is a leading systems integrator of COTS and custom products, with a proven track record in providing end-to-end, mission-critical health information technology (IT) solutions. Our professionals have vast experience in improving quality and efficiency across the fast-paced and dynamic healthcare continuum. Based on our in-depth understanding of CMS and our federal policy experience gained from our eight federal prime contracts, we will apply best practices, innovations, and solutions while maintaining compliance in our product and service delivery.

NewWave provides various project management and technical support services for CMS in executing the Medicaid and Children's Health Insurance Program Business Information Systems (MACBIS) program. NewWave, as systems integrator for the MACBIS enterprise suite of systems, works on behalf of CMS to ensure successful integration of five disparate enterprise systems into a single, data-driven analytic ecosystem—all while ensuring continuity of business operations across the enterprise.

NewWave is responsible for the largest healthcare claims data repository in the nation: the Chronic Condition Warehouse–Virtual Research Data Center (CCW-VRDC). Our unique Statistical Analysis System (SAS) grid-based software environment enables 1,000 researchers to build and run software code against Medicare and Medicaid claims data from as far back as 1991.

Our work in developing, managing, and modernizing the CMS Risk Adjustment Data Validation Centralized Data Abstraction Tool (RADV-CDAT) enables medical agencies to download instructions and data, complete coversheets, submit medical records, and view audits related to payment error rates for Medicare Part C reimbursement.

With our Enterprise Privacy Policy Engine (EPPE) work, NewWave provides a modernized, automated data use agreement process to streamline document scanning and sharing. NewWave integrates systems seamlessly using proven processes, including Project Management Institute (PMI), Capability Maturity Model Integration (CMMI), and Scaled Agile/Scrum methodologies.

As part of our Transformed Medicaid Statistical Information System (T-MSIS) contract, NewWave also provides IT technical assistance and support services to all 50 State Medicaid Agencies (SMA) plus the District of Columbia, enabling them to implement requirements, processes, business rules, and data conversion plans to meet T-MSIS reporting requirements. Services focus on managing bi-directional communication between Centers for Medicaid and CHIP Services (CMCS) and the states so that states properly receive federal messaging, and CMCS understands the individual states' circumstances.

Based on our efforts on programs such as the CMS-sponsored Provider Screening Challenge (PSC) program, NewWave has experience ensuring provider integrity and quality management for the states' Medicaid provider enrollment and screening processes. This program was a partnership between the U.S. Department of Health and Human Services, (HHS), CMS, National Aeronautics and Space Administration (NASA), MITRE, NewWave, and the State of Minnesota to develop a provider screening and enrollment system that meets state provider integrity requirements and verifies provider identity, credentials, and Medicaid eligibility. CMS created the Provider Screening Challenge to provide states with the information they need to establish the project management and technical foundation to modify and implement a successful Provider Screening System. The CMS project invited a "community of solvers" to produce innovative and creative solutions that deliver reliable, scalable, and economic provider screening capabilities for multiple states and federal health programs.

IBM is the largest technology and consulting employer in the world and a leading provider of social program management solutions. The IBM Cúram Social Program Management Platform (SPMP), which is part of IBM Watson Health, is built on a strong foundation of domain expertise and experience that touches the lives of people and families around the globe. Today, IBM Cúram Social Program Management operates in 50 Health and Human Services agencies across 18 countries supporting over 50 government programs.

Cúram is used by 280,000 case workers and protects more than 57 million clients annually. Cúram's self-service capabilities support 65 million people worldwide in 13 different languages. Since releasing Cúram version 1.0 in 1990, over 2,500 developer years have been invested in its seven subsequent releases, leading to a highly stable and mature health IT platform. IBM Watson Health analytics provides market-leading performance improvement solutions built on data integrity, advanced analytics, and domain expertise. IBM not only has a stable COTS product for the social services industry, but also has a solid analytics methodology. IBM's insights and solutions have been providing employers and health plans, state and federal government agencies, and policymakers with the facts they need to make confident decisions that directly affect the health and well-being of people and organizations in the United States and around the world.

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

Acronym/Abbreviation	Expansion/Definition
ACES	Automated Case Management and Eligibility System
ACID	Atomicity, Consistency, Isolation, Durability
ADA	Americans with Disabilities Act
ADE	Application Development Environment
ADOA	Arizona Department of Administration
AHCCCS	Arizona Health Care Cost Containment System
ANSI	American National Standards Institute
API	Application Programming Interface
APM	Application Performance Monitoring
ARS	Acceptable Risk Safeguards
ASET	Arizona Strategic Enterprise Technology
ATO	Authority to Operate
BAA	Business Associate Agreement
BI	Business Intelligence
BIRT	Business Intelligence and Reporting Tools; an open-source reporting technology with which Cúram integrates
BPEL	Business Process Execution Language
BPO	Business Process Object
BPR	Business Process Redesign
BPSSM	Business Partner System Security Manual
CADG	Cúram Analysis Documentation Generator
CAP	Corrective Action Plan
CARES	Client Assistance and Rehousing Enterprise System
CAS	Children Aid Societies
CCW	Chronic Condition Warehouse
CCW-VRDC	Chronic Condition Warehouse–Virtual Research Center
CDAT	Clinical Data Abstraction Tool
CEO	Chief Executive Officer
CER	Cúram Express Rules
CFACTS	CMS FISMA Control Tracking System
CHIP	Children's Health Insurance Program
CI/CD	Continuous Integration/Continuous Delivery
CISO	Chief Information Security Officer
CM	Configuration Management
CMMI	Capability Maturity Model Integration
CMS	Centers for Medicare and Medicaid
CON	Contract
COTS	Commercial Off-the-Shelf
CP	Contingency Plan
CPIN	Child Protection Information Network
CRD	Clinical Resource Directory

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

CPM	IBM Cúram Provider Management
CPU	Central Processing Unit
CSV	Comma Separated Values
CVO	Credentialing and Verification Organization
CYSSC	Children Youth and Social Services I&IT Cluster
Dev.	Development
DDI	Design, Development, and Implementation
DFDL	Data Format Description Language
DMP	Data Management Plan
DNS	Domain Name System
DOITT	Department of Information Technology and Telecommunications (New York City)
DOM	Document Object Model
DR	Disaster Recovery
DSG	Data and Systems Group
DUA	Data User Agreement
ECM	Enterprise Content Management
EDI	Electronic Data Interface
EIS	Eligibility Information Services
EPLS	Excluded Parties List System (now known as System for Award Management [SAM])
EPPE	Enterprise Privacy Policy Engine
ESB	Enterprise Service Bus
ESSO	Enterprise Single Sign-on
ETC	Estimate to Complete
EVM	Earned Value Management
FAQ	Frequently Asked Questions
FEA	Federal Enterprise Architecture
FHA	Federal Health Architecture
FIPS	Federal Information Processing Standard
FTI	File Type Information
FTP	File Transfer Protocol
HCC	Hierarchical Condition Category
HCR	Health Care Reform
HHS	U.S. Department of Health and Human Services
HHSC	Health and Human Services Commission
HIE	Health Information Exchange
HIPAA	Health Insurance Portability and Accountability Act
HIS	Hospital Information System
HITECH	Health Information Technology for Economic and Clinical Health (HITECH) Act
HL7	Health Level Seven International
HTML	Hypertext Markup Language
HTTPD	Hypertext Transfer Protocol Daemon (web server)
HTTPS	Hypertext Transfer Protocol Server
IaaS	Infrastructure as a Service

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

IAPD	Implementation Advance Planning Document
IBM	International Business Machines
IBM MQ	International Business Machines Message Queue
ID	Identification
IDS	Integrated Decision Support
IEG	Intelligent Evidence Gathering
IEPD	Information Exchange Package Documentation
IHSS	Integrated Human Services System (New York City)
IIB	IBM Integration Bus
IMS	Integrated Management System
Int	Integration
ISA	Interoperability Standards Advisory
ISO	International Standards Organization
ISP	Internet Service Provider
IT	Information Technology
ITIL	Information Technology Infrastructure Library
IV&V	Independent Verification and Validation
JAB	Joint Authorization Board
JAMIS	Joint Application Management Information System
JIRA	A truncation of Gojira, the Japanese name for Godzilla. Jira is a tool used for bug tracking, issue tracking, and project management, developed by Australian Company Atlassian.
JMS	Java Messaging Services
JSON	JavaScript Object Notation
JWT	Java Web Token
KMS	Knowledge Management System
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LEIE	List of Excluded Individual/Entities
LIS	Low Income Subsidy
MA	Medicare Advantage
MAO	Medicare Advantage Organization
MCBS	Medicare Current Beneficiary Survey
MACBIS	Medicaid and Children's Health Insurance Program Business Information Systems
MACBIS SI	Medicaid and Children's Health Insurance Program Business Information Systems System Integrator
MAG	Microsoft Azure for Government
MCO	Managed Care Organization
MCYS	Ministry of Children and Youth Services (Ontario)
MECL	Medicaid Enterprise Certification Life Cycle
MECT[1]	Medicaid Enterprise Certification Toolkit
MFA	Multi-factor Authentication
MITA	Medicaid Information Technology Architecture
MMIS	Medicaid Management Information System
MR	Medical Record

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

MS	Microsoft
NASA	National Aeronautics and Space Administration
NAT	National
NC FAST	North Carolina Families Accessing Services through Technology
NIEM	National Information Exchange Model
NIST	National Institute of Standards and Technology
NIST SP	National Institute of Standards and Technology Special Publication
NPI	National Provider Identifier
NPPES	National Plan and Provider Enrollment System
NSG	Network Security Group
NUCC	National Uniform Claim Committee
OACAS	Ontario's Association of Children's Aid Societies
OATH	Google Authenticator
OHA	Office of Hearings and Appeals
OOTB	Out-of-the-Box
ORR	Operational Readiness Review
OS	Operating System
PAPD	Planning Advance Planning Document
PCR	Priority, Complexity, and Risk
PDF	Portable Document Format
PECOS	Provider Enrollment, Chain and Ownership System (Medicare provider online enrollment system)
PHI	Protected Health Information
PI	Program Integrity
PII	Personally Identifiable Information
PMBOK	Project Management Book of Knowledge
PMI	Project Management Institute
PMO	Project Management Office
PMP	Project Management Plan
PMS	Provider Management System
PPQA	Process and Product Quality Assurance
PQPMI	Physician Quality Program Management Implementation
PRTG	Paessler Router Traffic Grapher
PSC	Provider Screening Challenge
PSTG	Private Sector Technology Group
PWP	Project Workplan
QA	Quality Assurance
QIO	Quality Improvement Organizations
QMO	Quality Management Office
RA	Remittance Advice
RACI	Responsible, Accountable, Consulted, and Informed
RADV CDAT	Risk Adjusted Data Validation Clinical Data Abstraction Tool
RAM	Responsibility Assignment Matrix
RASIC	Responsible, Approving, Supporting, Informed and Consulted—an employee uses these

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

	designations to define their relationship to parties for different parts of a project or corporation
RFP	Request for Proposal
RSA	IBM Rational Software Architect
RTM	Requirements Traceability Matrix
SAFe	Scalable Agile Framework
SAM	(IBM) Security Access Manager
SAML	Security Assertion Markup Language
SAS	Statistical Analysis System
SaaS	Software-as-a-Service
SCA	Security Controls Assessment
SCM	Software Configuration Management
SDD	Software Design Description
SDLC	Software Development Life Cycle
SIEM	Security Information and Event Management System
SIS	Single Information System
SLA	Service Level Agreement
SNAP	Supplemental Nutrition Assistance Program
SNMP	Simple Network Management Protocol
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SOW	Statement of Work
SPIP	Software Process Improvement Plan
SPM	Social Program Management
SPMP	Social Program Management Platform
SQL	Structured Query Language
SS-A	State Self-Assessment
SSI	Supplemental Security Income
SSL	Secure Sockets Layer
SSO	Single Sign-on
SSP	System Security Plan
SWIFT	Society For Worldwide Interbank Financial Telecommunications
TLS	Transport Layer Security
T-MSIS	Transformed Medicaid Statistical Information System
TRA	Technical Reference Architecture
TSR	Test Summary Reports
UAT	User Acceptance Testing
UDDI	Universal Description, Discovery, and Integration
UI/UX	User Interface/User Experience
UML	Uniform Modeling Language
USDS	United States Digital Services
Val	Validation
VHD	Virtual Hard Drives
VPN	Virtual Private Network

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

VRDC	Virtual Research Data Center
VSTS	Microsoft's Visual Studio Team System
W3C	World Wide Web Consortium
WAI	Web Accessibility Initiative
WAN/WLAN	Wide Area Network/Wireless Local Area Network
WBS	Work Breakdown Structures
WCAG	Web Content Accessibility Guidelines
WSDL	Web Service Description Language
XML	eXtensible Markup Language
X12	American National Standards Institute Accredited Standards Committee electronic data interchange standard

Acronym/Abbreviation	Expansion/Definition
ACES	Automated Case Management and Eligibility System
ACID	Atomicity, Consistency, Isolation, Durability
ADA	Americans with Disabilities Act
ADE	Application Development Environment
ADOA	Arizona Department of Administration
AHCCCS	Arizona Health Care Cost Containment System
ANSI	American National Standards Institute
API	Application Programming Interface
APM	Application Performance Monitoring
ARS	Acceptable Risk Safeguards
ASET	Arizona Strategic Enterprise Technology
ATO	Authority to Operate
BAA	Business Associate Agreement
BI	Business Intelligence
BIRT	Business Intelligence and Reporting Tools; an open-source reporting technology with which Cúram integrates
BPEL	Business Process Execution Language
BPO	Business Process Object
BPR	Business Process Redesign
BPSSM	Business Partner System Security Manual
CADG	Cúram Analysis Documentation Generator
CAP	Corrective Action Plan
CARES	Client Assistance and Rehousing Enterprise System
CAS	Children Aid Societies
CCW	Chronic Condition Warehouse
CCW-VRDC	Chronic Condition Warehouse–Virtual Research Center
CDAT	Clinical Data Abstraction Tool

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

CEO	Chief Executive Officer
CER	Cúram Express Rules
CFACTS	CMS FISMA Control Tracking System
CHIP	Children's Health Insurance Program
CI/CD	Continuous Integration/Continuous Delivery
CISO	Chief Information Security Officer
CM	Configuration Management
CMMI	Capability Maturity Model Integration
CMS	Centers for Medicare and Medicaid
CON	Contract
COTS	Commercial Off-the-Shelf
CP	Contingency Plan
CPIN	Child Protection Information Network
CRD	Clinical Resource Directory
CPM	IBM Cúram Provider Management
CPU	Central Processing Unit
CSV	Comma Separated Values
CVO	Credentialing and Verification Organization
CYSSC	Children Youth and Social Services I&IT Cluster
Dev.	Development
DDI	Design, Development, and Implementation
DFDL	Data Format Description Language
DMP	Data Management Plan
DNS	Domain Name System
DOITT	Department of Information Technology and Telecommunications (New York City)
DOM	Document Object Model
DR	Disaster Recovery
DSG	Data and Systems Group
DUA	Data User Agreement
ECM	Enterprise Content Management
EDI	Electronic Data Interface
EIS	Eligibility Information Services
EPLS	Excluded Parties List System (now known as System for Award Management [SAM])
EPPE	Enterprise Privacy Policy Engine
ESB	Enterprise Service Bus
ESSO	Enterprise Single Sign-on
ETC	Estimate to Complete
EVM	Earned Value Management
FAQ	Frequently Asked Questions
FEA	Federal Enterprise Architecture
FHA	Federal Health Architecture
FIPS	Federal Information Processing Standard
FTI	File Type Information

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

FTP	File Transfer Protocol
HCC	Hierarchical Condition Category
HCR	Health Care Reform
HHS	U.S. Department of Health and Human Services
HHSC	Health and Human Services Commission
HIE	Health Information Exchange
HIPAA	Health Insurance Portability and Accountability Act
HIS	Hospital Information System
HITECH	Health Information Technology for Economic and Clinical Health (HITECH) Act
HL7	Health Level Seven International
HTML	Hypertext Markup Language
HTTPD	Hypertext Transfer Protocol Daemon (web server)
HTTPS	Hypertext Transfer Protocol Server
IaaS	Infrastructure as a Service
IAPD	Implementation Advance Planning Document
IBM	International Business Machines
IBM MQ	International Business Machines Message Queue
ID	Identification
IDS	Integrated Decision Support
IEG	Intelligent Evidence Gathering
IEPD	Information Exchange Package Documentation
IHSS	Integrated Human Services System (New York City)
IIB	IBM Integration Bus
IMS	Integrated Management System
Int	Integration
ISA	Interoperability Standards Advisory
ISO	International Standards Organization
ISP	Internet Service Provider
IT	Information Technology
ITIL	Information Technology Infrastructure Library
IV&V	Independent Verification and Validation
JAB	Joint Authorization Board
JAMIS	Joint Application Management Information System
JIRA	A truncation of Gojira, the Japanese name for Godzilla. Jira is a tool used for bug tracking, issue tracking, and project management, developed by Australian Company Atlassian.
JMS	Java Messaging Services
JSON	JavaScript Object Notation
JWT	Java Web Token
KMS	Knowledge Management System
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LEIE	List of Excluded Individual/Entities
LIS	Low Income Subsidy

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

MA	Medicare Advantage
MAO	Medicare Advantage Organization
MCBS	Medicare Current Beneficiary Survey
MACBIS	Medicaid and Children's Health Insurance Program Business Information Systems
MACBIS SI	Medicaid and Children's Health Insurance Program Business Information Systems System Integrator
MAG	Microsoft Azure for Government
MCO	Managed Care Organization
MCYS	Ministry of Children and Youth Services (Ontario)
MECL	Medicaid Enterprise Certification Life Cycle
MECT[1]	Medicaid Enterprise Certification Toolkit
MFA	Multi-factor Authentication
MITA	Medicaid Information Technology Architecture
MMIS	Medicaid Management Information System
MR	Medical Record
MS	Microsoft
NASA	National Aeronautics and Space Administration
NAT	National
NC FAST	North Carolina Families Accessing Services through Technology
NIEM	National Information Exchange Model
NIST	National Institute of Standards and Technology
NIST SP	National Institute of Standards and Technology Special Publication
NPI	National Provider Identifier
NPPES	National Plan and Provider Enrollment System
NSG	Network Security Group
NUCC	National Uniform Claim Committee
OACAS	Ontario's Association of Children's Aid Societies
OATH	Google Authenticator
OHA	Office of Hearings and Appeals
OOTB	Out-of-the-Box
ORR	Operational Readiness Review
OS	Operating System
PAPD	Planning Advance Planning Document
PCR	Priority, Complexity, and Risk
PDF	Portable Document Format
PECOS	Provider Enrollment, Chain and Ownership System (Medicare provider online enrollment system)
PHI	Protected Health Information
PI	Program Integrity
PII	Personally Identifiable Information
PMBOK	Project Management Book of Knowledge
PMI	Project Management Institute
PMO	Project Management Office
PMP	Project Management Plan

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

PMS	Provider Management System
PPQA	Process and Product Quality Assurance
PQPMI	Physician Quality Program Management Implementation
PRTG	Paessler Router Traffic Grapher
PSC	Provider Screening Challenge
PSTG	Private Sector Technology Group
PWP	Project Workplan
QA	Quality Assurance
QIO	Quality Improvement Organizations
QMO	Quality Management Office
RA	Remittance Advice
RACI	Responsible, Accountable, Consulted, and Informed
RADV CDAT	Risk Adjusted Data Validation Clinical Data Abstraction Tool
RAM	Responsibility Assignment Matrix
RASIC	Responsible, Approving, Supporting, Informed and Consulted—an employee uses these designations to define their relationship to parties for different parts of a project or corporation
RFP	Request for Proposal
RSA	IBM Rational Software Architect
RTM	Requirements Traceability Matrix
SAFe	Scalable Agile Framework
SAM	(IBM) Security Access Manager
SAML	Security Assertion Markup Language
SAS	Statistical Analysis System
SaaS	Software-as-a-Service
SCA	Security Controls Assessment
SCM	Software Configuration Management
SDD	Software Design Description
SDLC	Software Development Life Cycle
SIEM	Security Information and Event Management System
SIS	Single Information System
SLA	Service Level Agreement
SNAP	Supplemental Nutrition Assistance Program
SNMP	Simple Network Management Protocol
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SOW	Statement of Work
SPIP	Software Process Improvement Plan
SPM	Social Program Management
SPMP	Social Program Management Platform
SQL	Structured Query Language
SS-A	State Self-Assessment
SSI	Supplemental Security Income
SSL	Secure Sockets Layer

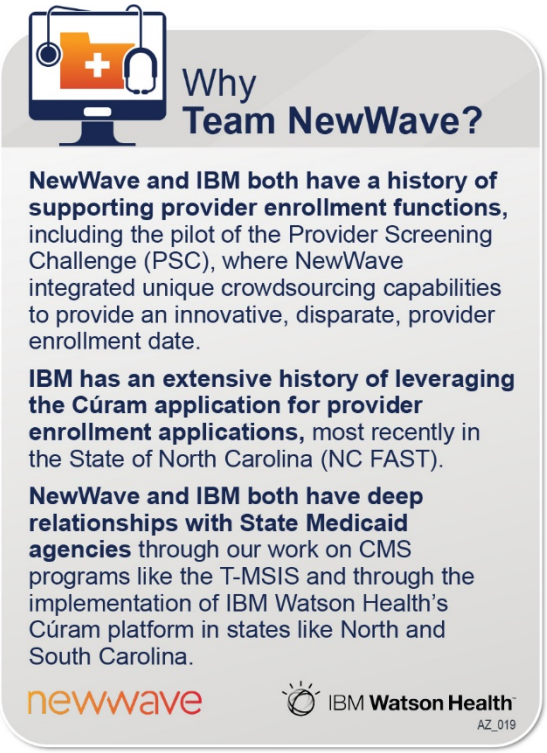
Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

SSO	Single Sign-on
SSP	System Security Plan
SWIFT	Society For Worldwide Interbank Financial Telecommunications
TLS	Transport Layer Security
T-MSIS	Transformed Medicaid Statistical Information System
TRA	Technical Reference Architecture
TSR	Test Summary Reports
UAT	User Acceptance Testing
UDDI	Universal Description, Discovery, and Integration
UI/UX	User Interface/User Experience
UML	Uniform Modeling Language
USDS	United States Digital Services
Val	Validation
VHD	Virtual Hard Drives
VPN	Virtual Private Network
VRDC	Virtual Research Data Center
VSTS	Microsoft's Visual Studio Team System
W3C	World Wide Web Consortium
WAI	Web Accessibility Initiative
WAN/WLAN	Wide Area Network/Wireless Local Area Network
WBS	Work Breakdown Structures
WCAG	Web Content Accessibility Guidelines
WSDL	Web Service Description Language
XML	eXtensible Markup Language
X12	American National Standards Institute Accredited Standards Committee electronic data interchange standard

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

TAB A. PROPOSED METHOD OF APPROACH

NewWave Telecom & Technologies, Inc. (NewWave) has extensive experience in providing information technology (IT) technical assistance and support services to all 50 State Medicaid Agencies (SMA), plus the District of Columbia as well as the Centers for Medicare and Medicaid Services (CMS). We also are involved in provider integrity and quality management of Medicaid provider enrollment and screening processes with the State of Minnesota. NewWave has partnered with IBM Watson Health to develop and present a solution for the Arizona Health Care Cost Containment System (AHCCCS) and Hawaii's Med-QUEST Provider Management System (PMS).



To meet the state's provider management requirements, the solution will consist of IBM Cúram Intake and Assessment, IBM Cúram Appeals and Legal Action, and IBM Cúram Service Provider Management modules. These commercial off-the-shelf (COTS) products, in combination with other system components, can be configured to meet the needs of Arizona and Hawaii. Team NewWave will provide full lifecycle support and iteratively develop and release updates in coordination with business owners from the respective clients.

For the PMS, Team NewWave selected IBM's internationally successful IBM Cúram Social Program Management Platform (SPMP), reflecting over 20 years of enhancements providing the most stable, extensible COTS social program management solution available. Team NewWave understands the challenges health and human services agencies face with customized legacy systems, costly and proprietary interfaces, and ongoing system modifications. To address these challenges, and to ensure AHCCCS/Med-QUEST receives a provider enrollment system that meets current and future demands with minimal cost, disruption, and minimal learning curve, Team NewWave proposes a solution based on the IBM Cúram SPMP. Cúram is a COTS platform that aligns new technology with policy objectives and technology initiatives designed specifically for social enterprises. IBM's Cúram is a mature, stable, and secure software solution.

Team NewWave's COTS solution, summarized in Figure 1, is hosted in Microsoft's Azure Cloud Services, a Federal Risk and Authorization Management Program (FedRAMP)–authorized Infrastructure-as-a-Service (IaaS) platform that meet the Health Insurance Portability and Affordability Act (HIPAA) control requirements. Cúram delivers role-specific home pages and displays dashboards that show real-time system data. It provides a 360-degree view of providers, with the option to scale and increase functionality with new modules.

IBM's Cúram, a highly scalable and reliable COTS front-end provider management enrollment solution, eliminates barriers to enrollment and empowers users with an easy-to-use, interoperable, multi-access, and streamlined platform without unnecessary duplication. Cúram's recently released Version 7 (v.7.0.2), an industry-proven extensible solution with generations of enhancements that enable modularity, reuse, and shared services without extensive development effort. With its comprehensive set of leading practices, business processes, and service delivery models, Cúram supports end-to-end program and service delivery to over 50 government programs in 18 countries.

North Carolina's Department of Health and Human Services' North Carolina Families Accessing Services through Technology (NC FAST) program successfully implemented the IBM Cúram solution. In 2013, NC FAST subsequently implemented Cúram to process Medicaid applications. NC FAST now supports enrollment for different provider types, including Medicaid, subsidized childcare, energy, and child welfare providers.

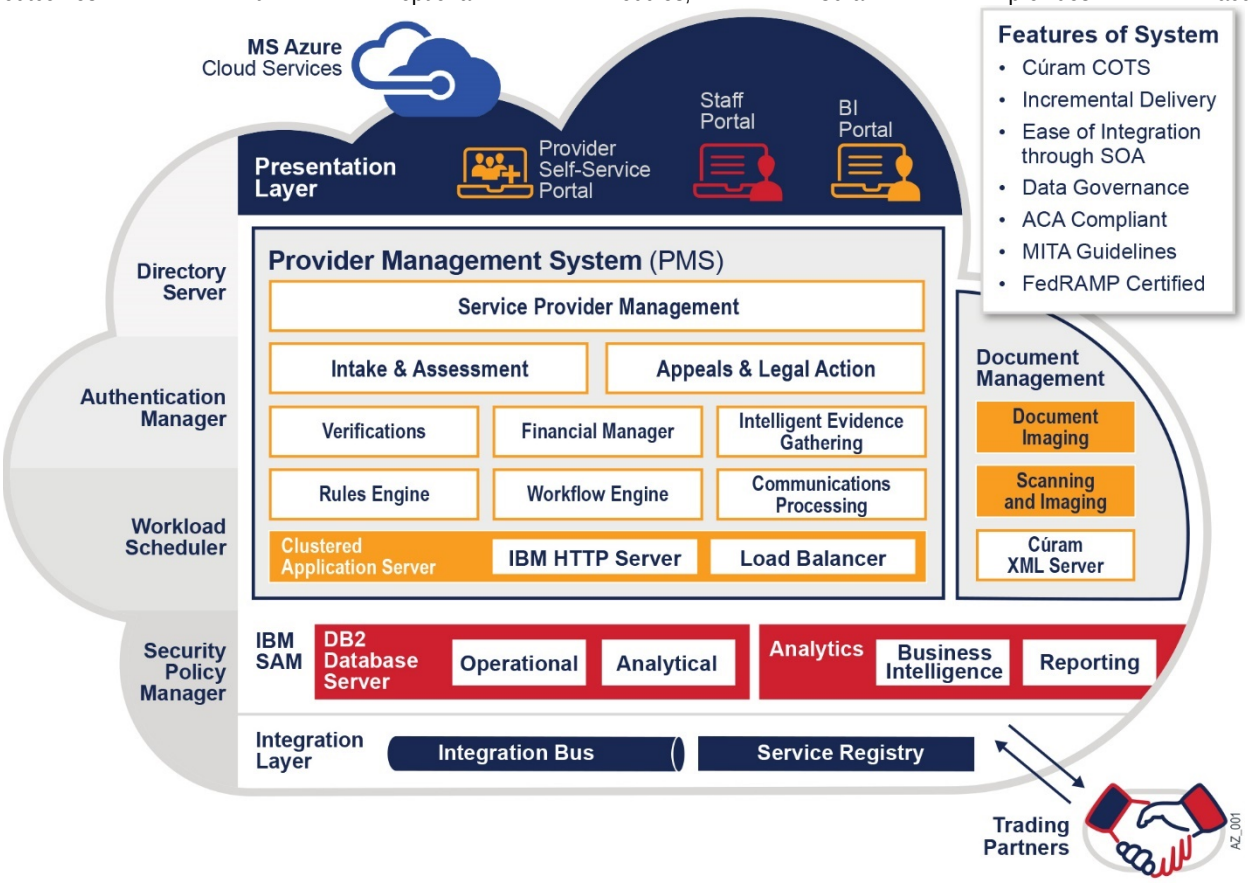
Minnesota's Eligibility Technology System (MN METS) is another example of how we were able to support many health and human services programs with our COTS provider management solution. Using the IBM Cúram Service Provider Management module, MN METS facilitates the registration and maintenance processes for several provider types, including Navigators, Assistors, and Brokers. Providers access MN METS via a secure portal, which enables them to manage their clients. Navigators,

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

Assistors, and Brokers also assist clients through the application process, answering questions about the process as well as the services they provide.

Figure 1: Team NewWave's Provider Management Solution

To meet today's most vexing healthcare challenges, state healthcare organizations need to become data-driven; they need to handle ever-greater data volume and variety to provide data-driven decision-making that drives and improves business outcomes. With optional modules, Cúram provides acc



ess to IBM's Watson, a powerful cognitive analytic computing platform that will enable Team NewWave to address program integrity using advanced analytics, to create new approaches for value creation, and to deliver outcome-driven performance using machine language as part of the cognitive services.

With our long-standing IBM partnership, Team NewWave has vast experience in integrating IBM's cutting-edge solutions that will enable AHCCCS/Med-QUEST to harness the functional capacity of Cúram's flexible, modular architecture options to address growth and changes to federal and state-specific requirements.

A.1 Overall Requirements (SOW 5.1)

Arizona and Hawaii each have business owners who have different business processes and requirements. We have experienced this situation with many of our clients, and we have the experience and expertise to support two instances of the solution with state-specific workflow configurations, security, and databases for segregation of the data. There will be two instances of each interface, one for each state, and support will be provided in two different time zones.

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

Our approach supports the ability to migrate data out of the cloud into each state's data centers in the future. Section A.18, Project Management details our approach timeline and milestones; we are working on data from Day 1, determining the data source and mapping to begin data conversion.

SOW	Team NewWave Response
5.1.1	Team NewWave's proposed solution is based on IBM Cúram Service Provider Management. Cúram is a COTS platform that aligns new technology with policy objectives and technology initiatives designed specifically for social enterprises. IBM's Cúram is a mature, stable, and secure software and operational development platform that is currently on Version 7.0.2. Cúram has been determined to be an acceptable COTS product that is compliant with all federal rules and has been approved for funding by the Department of Agriculture and the Department of Health & Human Services.
5.1.2	Our proposed solution involves configuring a guided, wizard-driven application for the enrollment application. We follow a similar guided process for re-enrollment, recertification, and revalidation; however, these scripts can be pre-populated with available provider enrollment data to expedite the process and to increase the accuracy of the data received. Providers will also have the ability to complete a termination request from their secure account. The portal is a responsive web-based portal that supports access from cell phones, tablets, and PCs. Appendix A, Figure 12, shows an example of a guided process for enrollment. The provider can click NEXT and/or BACK to navigate the application; the blue progress bar on top shows the overall progress through the application process. Real-time notification is provided by a confirmation message once the provider submits the application, and an email is sent to the provider's email address.
5.1.3	Team NewWave's solution enables agencies to holistically manage the details of providers, the services they provide, and financial details related to those services. Additional provider details are tracked, including facilities, service locations, provider credentials, contracts, ownership, and additional provider member details, as shown in Appendix A, Figure 13, Provider Home Page. Using IBM Cúram Service Provider Management, Team NewWave's solution also captures details related to provider claims and service authorizations, and additional details to be determined by the state.
	Testing here Try again Testing here again
5.1.4	The portal offers interactive online support during the enrollment process by visually indicating error conditions to the providers and suggesting means for correcting the errors the provider may encounter on a page. If the provider is unable to continue, a FAQ-style help page is available to the provider. Also, the provider may submit online questions through the portal. These questions are sent to an inbox where an internal worker has the capability to respond to the provider. The portal also makes contact information available if the provider is unable to proceed using the various self-help tools available. If desired, Team NewWave will integrate into the provider portal a real-time interactive Chatbot using IBM Watson cognitive services. Watson Support Chatbots are built to master a single domain; they walk a user through any major business processes and answer a wide range of FAQ-type questions.
5.1.5	Our proposed solution will retain versions of documents published on the platform. Team NewWave also will implement a database backup policy that includes daily incremental backup, weekly full backup, and monthly full backup. These backups enable recovery to any day of the year.
5.1.6	The PMS portal gives the provider a wizard-like guided experience through the application process. On completion of

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

SOW	Team NewWave Response
	the application, the provider is directed to a page where they can upload documents from their secure online account based on the services the provider requested. An example list of required documents is shown in Appendix A, Figure 14. This list is derived from the list of outstanding verification items on their application. The provider is presented with a list of outstanding items for verification and can select items to upload based on the missing items. An additional feature enables the provider to upload state-required documents that are not related to outstanding verifications. Both lists are maintained in the provider's account, along with the document status. Workflows are enacted when documents are uploaded, and a task is sent to a user to accept or reject the documents.
5.1.7	Team NewWave's solution's platform will recognize all types of electronic document format types supported by Arizona and Hawaii. There are no restrictions imposed on electronic document formats.
5.1.8	Team NewWave's solution includes the Cúram Supervisor Workspace, which presents supervisors with workload information for each work queue. It enables users to view the system workload and helps supervisors make better, data-driven decisions through: (1) supervisor dashboard views of work queues and user assignments; (2) real-time display and access to information; (3) centralized management of applications and tasks; (4) workload prioritization, balancing, and allocation; and (5) management of work processes across multiple levels of the agency. Using IBM Supervisor Workspace enables users to efficiently track, manage, and oversee work queues and task status across all areas of the solution.
5.1.9	Team NewWave will deploy the new solution in the Microsoft Azure for Government (MAG) data center located in Arizona. NewWave is a leader in cloud technology implementation and will ensure efficient utilization of cloud resources.
5.1.10	MAG is a virtualized IaaS. The PMS will be installed on virtual machines, which can be migrated to AHCCCS/Med-QUEST virtual environments by copying the virtual hard drives and configurations.
5.1.11	On completion of the application for enrollment, reenrollment, revalidation, or recertification, the provider is directed to a page of outstanding items to complete. This includes affirmation, and signature if the state desires, of the Provider Participation Agreement. The provider is presented with the language of the provider agreement as directed by the State and is given the opportunity to sign the agreement digitally. Once the provider signs or affirms the agreement, the outstanding item is marked as completed on the provider's list and the agreement and signature is attached to the provider record.
5.1.12	All system documentation will be complete for the operational readiness review (ORR) and Medicaid Information Technology Architecture (MITA) certification. The documentation will provide enough detail so that any technical team can take over operations and hosting by consulting the technical documents.
5.1.13	Team NewWave will manage and ensure that virtual machines are updated according to the security guidelines. MAG follows the strictest security guidelines and the hardware is updated and upgraded according to Microsoft's industry-leading service level agreements (SLA). Team NewWave's solution is highly scalable. Our Change Control policy ensures that all upgrades are deployed with no user impact. IBM Cúram is designed to be customizable and upgradable by projects and there are published guidelines on how to design and develop custom extensions to the product. Cúram also has a schedule of releases and enhancements to the product. IBM Cúram also publishes an Upgrade Helper tool to assist in upgrading the software and database, while maintaining all project-level extensions. For more information on the Upgrade Helper tool, see our response to SOW 5.21.1.
5.1.14	All system users, including providers, interact with our solution using a standard web browser. Internal users use an internal-facing website. On login, users are directed to a home page configured for their specific role. An example home page is shown in Appendix A, Figure 15 Enrollment Specialist Dashboard. Providers interact with a public-facing website (using secure login credentials to access personal information). Appendix A, Figure 16 Provider Poral Home Page, depicts an example of the provider's home page on login. Providers can access the website using a range of devices, including cell phones, tablets, and laptops, because the user interface is responsive and optimized for usage on the device. Providers do not require additional software to be

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

SOW	Team NewWave Response
	installed. System users can use tablets to access the web application, and it is supported by Cúram. For more information on tablet support, visit the Knowledge Center at https://ibm.biz/BdZ4sr. When using a desktop or laptop, system users may require an additional browser plugin such as Adobe Flash player. This technology is used in certain administrative functions. If a business user wishes to create or edit a Microsoft Word template from within the PMS, a Java browser plugin is required. These plugins are common technologies used by many robust web applications.
5.1.15	Team NewWave will develop system architecture documentation following ITIL, CMS well-architected framework, MITA architectural guidelines, and industry best practices. These will include data and application flow diagrams, all subsystem and component specifications, including all COTS and software-as-a-service (SaaS) products and hosting details. This also includes all network configurations and interfaces.
5.1.16	A data dictionary will be created that defines all Master Data, which will include identification of sources, origin, and field-level format of each data point. Database documentation also includes schemas and data infrastructure configurations. Team NewWave will create detailed documentation of all interfaces with other systems, including data format and transformations performed on data sent or received.
5.1.17	All system data are stored in a central DB2 database that will be located in the MAG data center in Arizona, a passive disaster recovery (DR) site will be MAG in Virginia, and a third offline backup will be stored in Iowa. No data will be stored outside the United States. AHCCCS and Med-QUEST sites and configurations will be segregated and can be modified independent of each other.
5.1.18	Both implementations of our solution maintain separate DB2 databases. These will be deployed on segregated network locations such that access can be limited to those working within AHCCCS or Med-QUEST, but no data can be transferred between implementations.
5.1.19	The solution accepts e-signatures in accordance with Arizona' and Hawaii's policy document. An example of e-signature usage is when the provider submits an application for enrollment from the provider portal; one of the final pages of the application is to explicitly provide identifying information and check a mandatory checkbox agreeing to terms and conditions and confirming identity. Any verbiage on this page is configurable and Team NewWave will work with the states to display the appropriate language. Once submitted, the record is stored against the application that was submitted and timestamped. The same process can be applied where needed. Also, if desired, the system can be integrated with another tool to capture digital signatures and apply that signature to the appropriate document. Team NewWave will work with the state to refine the requirements in this area.
5.1.20	All licenses will be procured and owned by AHCCCS and Med-QUEST. NewWave can procure them on behalf of the state; we provide the cost of these licenses in the proposal. NewWave can provide licenses within 30 days of request.
5.1.21	Team NewWave ensures that data integrity is maintained with an error rate less than 0.001% of transitions by monitoring and correcting data issues. Team NewWave will work to identify all legacy data and ensure that data ingested into the new system meets business requirements and will thoroughly test data on an ongoing basis. We also will report any data integrity issues to the state immediately and work to correct any compromised data.
5.1.22	NewWave is a technical leader at CMS. Team NewWave proposes a solution that is in line with CMS Technical Reference Architecture (TRA) guidelines. We have been at the forefront of providing complex health IT system integration for federal and state health and human services. Some of our successful projects at CMS that required conformance with CMS TRA include the following: • Medicaid and Children's Health Insurance Program Business Information Systems System Integrator (MACBIS SI) • Chronic Condition Warehouse (CCW) • Enterprise Privacy Policy Engine (EPPE) • Risk Adjusted Data Validation Clinical Data Abstraction Tool (RADV CDAT).
5.1.23	Team NewWave's solution provides functionality that is consistent with MITA.

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

SOW	Team NewWave Response
5.1.24	Team NewWave sized our solution based on the numbers provided in the SOW and Amendment 1. Our solution is highly scalable and able to meet the demands of users at peak usage. Team NewWave will perform advanced load testing before going live to ensure our solution can be scaled to meet demand. The Azure hosting platform ensures that sufficient hardware resources are available to the solution application based on its auto-scale capabilities, which can scale up or scale down based on usage. The web applications will be deployed in a WebSphere clustered environment where additional cluster members can be added or removed based on the system demands. Load balancers are used to ensure requests are routed to the appropriate resource to prevent overloading of any single resource. Combining multiple components with load balancing eliminates a single point of failure, which increases system reliability and availability. It also ensures the entire solution is highly scalable and performs for all system users. Government agencies worldwide have implemented Cúram solutions. Implementations serve the needs of single to multiple government agencies assisting diverse populations, involve one or multiple programs, and support end-user populations ranging from fewer than 100 users to more than 475,000 users.
5.1.25	Team NewWave ensures there is less than 2 seconds of latency between transaction initiation and response for Enterprise Service Bus (ESB), and we deploy advanced monitoring tools to ensure we meet this SLA on an ongoing basis. The ESB will be deployed in a highly available configuration such that services can be failed over to another region to ensure the system meets the availability SLA.

A.2 Documentation and Certification (SOW 5.2)

SOW	Team NewWave Response
5.2.1	Team NewWave understands the importance of ensuring system documentation reflects the current state of the environment. See Section A.27 and the PMP for our Configuration and Change Control approach to the Provider Management System and its documentation.
5.2.2	Team NewWave understands the importance of ensuring functional and user documentation reflects the current operations of the system. See Section A.27 and the PMP for our Configuration and Change Control approach to the Provider Management System and its documentation.
5.2.3	Team NewWave will provide all licenses required for AHCCCS/Med-QUEST and Medicaid providers to perform their work. This is a common practice for NewWave and our partner IBM. See our response to SOW 5.1.20 regarding licensing and our separate Business Volume for specific pricing.
5.2.4	Team NewWave ensures our solution meets the federal standards, conditions, and business requirements necessary for AHCCCS/Med-QUEST to receive CMS certification and will continue to maintain our solution in accordance with CMS requirements. See Section A.27 for a detailed description of our approach.

A.3 Regulatory System Compliance (SOW 5.3)

SOW	Team NewWave Response
5.3.1	Team NewWave's solution complies with the system requirements and standards as designated in the Medicaid Manual, Part 11. We will design our solution in accordance with the provider subsystem requirements outlined by facilitating enrollment of qualified providers on agreement of the rules and regulations of the state Medicaid program. This solution ensures that providers are qualified through a thorough screening method, processing provider applications and changes in a timely fashion, maintaining all data related to provider enrollment, and periodically re-verifying provider eligibility. The solution will also comply with the standards outlined in Subtitle F of Public Law 104-19 that pertain to electronic transactions, code sets, unique identifiers, security of health information, and electronic signatures. The solution also will adhere to state's performance standards.
5.3.2	The Cúram browser-based user interface is designed to be accessible so that persons with disabilities can use Cúram solutions effectively. Cúram conforms to both the U.S. Section 508 requirements for accessibility for persons with disabilities and the Americans with Disabilities Act (ADA). Cúram has been tested using the World Wide Web Consortium (W3C) Web Content Accessibility Guidelines 2.0 (WCAG 2.0).

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

SOW	Team NewWave Response
	The WCAG 2.0 technical guidelines are developed by the Accessibility Guidelines Working Group as part of the Web Accessibility Initiative (WAI); Cúram is currently Level AA compliant with WCAG 2.0, with minor exceptions on tablet devices.
5.3.3	Team NewWave will comply with all state and federal data requirements, including those established for Quality Improvement Organizations (QIOs) under the Title XI of the Affordable Care Act (ACA).
5.3.4	Team NewWave will be responsible for the PMS's federal certification plan, which will capture all necessary data and information and will be provided for CMS review before the scheduled CMS onsite visit. We understand CMS' criteria for federal certification as defined by the Medicaid Enterprise Certification Toolkit (MECT) and the development of the MECT artifacts (MECT 2_2 Appendix B Required Artifacts List) for the PMS. Team NewWave is familiar with the Medicaid Enterprise Certification Life Cycle. Previous systems we have supported, such as Idaho, Maine, North Carolina, and South Carolina, were certified after development was completed, but the CMS MECT 2_2 certification activities are performed at various milestone reviews. We will begin planning and capturing required documentation at the beginning of our implementation process and continue throughout the operations phase. Please refer to Section A.27 for additional details.
5.3.5	Pursuant to 42 CFR 455.436, our solution automates routine checks to determine the exclusion status of providers against federal databases, including the following: • Social Security Administration's Death Master File • National Plan and Provider Enumeration System (NPPES) • List of Excluded Individuals/Entities (LEIE) • System for Award Management (SAM), formerly Excluded Parties List System (EPLS) Checks against LEIE and SAM will occur no less frequently than monthly.
5.3.6	Team NewWave will use the automated tools and capabilities of our proposed solution to track and report licensing usage and expirations. Any renewals required will be reported to AHCCCS/Med-QUEST at least 180 days before the expiration date.
5.3.7	Team NewWave will comply with the relevant sections of the ACA. Examples of compliance include using inter-operable standards and formats through the Enterprise Service Bus (ESB) pattern and data transformation, which enable adherence to National Information Exchange Model (NIEM) standards; the use of both real-time and offline electronic interfaces to systems such as NPPES, LEIE, or EPLS to enable provider matching; and the capability for providers to upload digital documents from the provider portal to simplify the enrollment process.
5.3.8	The system will comply with standards adopted by the Secretary under Section 1104 of the ACA. This is accomplished by supporting the acceleration of HHS adoption of uniform standards and operation rules for the electronic transactions that occur between providers and health plans that are governed under HIPAA. The result is a reduction in the clerical burden on providers, patients, and health plans.
5.3.9	Cúram's accessibility compliance with ADA Section 508 accessibility standards is described in SOW 5.3.2.
5.3.10	Cúram Express Rules (CER) is based on a technology-neutral XML format with an associated schema document. The CER architecture has the capability to interoperate with other published data formats such as NIEM by consuming or producing data formatted using the core NIEM data elements. For a detailed description of Cúram business rules, see Team NewWave's response to SOW 5.4.3. Our response to this requirement was written in consideration of Q&A document item #171.
5.3.11	Team NewWave's solution is based on service-oriented architecture (SOA) with the following principles: • Service Structure and Invocation • Enterprise Service Bus • Orchestration and Composition • Standards-Based Data Exchange • Integration of Legacy Systems. All SOA services will be documented and exposed using Web Service Description Language (WSDL) and industry

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

SOW	Team NewWave Response
	best practices.
5.3.12	There are myriad federal laws, regulations, guidance, and standards concerning handling and exchanging of personally identifiable information (PII), personal health information (PHI), and the disclosure of file type information (FTI). There is no single, integrated, comprehensive approach to security and privacy that respects all potentially applicable federal requirements under the Federal Information Security Management Act (FISMA), HIPAA, Health Information Technology for Economic and Clinical Health (HITECH) Act, ACA, Tax Information Safeguarding Requirements, and state requirements. CMS' Harmonized Security and Privacy Framework provides a detailed definition of a common baseline of minimum acceptable risk controls requirements that support collaborative solutions to manage risks. Our proposed system will support security and privacy controls outlined in Harmonized Security and Privacy Frameworks, which include the following: • System and Data Classification • Security Controls • Identity, Credential, and Access Management • Secure Infrastructure and Managed Services Computing • Data Encryption • Audit Trails • Continuity of Operations and Disaster Recovery • Compliance Oversight • Privacy.
5.3.13	Team NewWave will incorporate Information Technology Infrastructure Library (ITIL) version 3 best practices for delivering and managing IT services during implementation and maintenance of our solution. Our CMMI Level 4-Services–appraised processes provide the framework for ensuring ITIL compliance.
5.3.14	The Web UI is in conformance with W3C standards and practices, and we will include routine validation against W3C Markup Validation Service.

A.4 System Architecture (SOW 5.4)

SOW	Team NewWave Response
5.4.1	The IBM Cúram Social Program Management Platform, the platform of Team NewWave's solution, incorporates extensive workflow management capabilities to support the automation of business processes. It enables agencies to define and maintain workflows to ensure best practices are followed and to improve the speed, consistency, and quality of business processing. Workflows are composed of activities and transitions, where each activity can be automatic or manual (requires human interaction). For example, the provider enrollment process initiates a workflow when an application is submitted. Some paths in the workflow may require a manual step of performing or documenting a site visit before the workflow can continue. Workflows also can participate in a Business Process Execution Language (BPEL) orchestrated process. This is done by providing functionality to expose Cúram workflow processes as web services that can be invoked from BPEL process partner links.
5.4.2	At the application level, Cúram transactions typically follow the optimistic locking pattern and transactions are bean-managed at the façade level, meaning the transaction begins when the user invokes a client-side operation. Optimistic locking ensures the atomicity, consistency, isolation, and durability (ACID) of transactions in Cúram, thus ensuring data integrity. Alternatively, each read transaction within Cúram can also be configured to obtain an exclusive update lock on the record that was read. These locks are not released until the end of the transaction. Team NewWave deploys advanced monitoring tools such that all transactional services, both internal and external, are monitored and alerts are generated if there are errors or delays in any service. This ensures that asynchronous transfers are completed successfully, and that messaging services and transactional processes are operating as expected. In the event of an outage, our technicians will work to restore the services by failing over to another

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

	highly available server within the same Azure region or will fail the entire system over to the passive Azure region. All transactions will be stored by Cúram or the ESB until they can be executed successfully; if asynchronous data are lost, Team NewWave will request that the interface group resend the data.
5.4.3	The solution's rules capability, referred to as Cúram Express Rules (CER), provides a highly versatile and adaptable rules environment that supports the definition, creation, and execution of rules to support a range of business functions commonly required by social enterprise agencies. CER consists of the Editor and Engine components, as follows: CER Editor: Provides a user-friendly tool for business analysts and developers to storyboard, design, and construct rules, and to link rules to data. It enables a business rules user to draw a set of rules diagrams, and to enable or disable existing rules, without programmer intervention, using an intuitive drag-and-drop approach. CER Engine: Executes rules on demand at runtime to output business-based calculations. CER Engine is a backward-chaining "calculation engine" that calculates "attributes." An attribute can be calculated from other attributes or from data on the Cúram data model or can be obtained from an external source. CER can be used to define and execute business calculations to support a range of rules-driven business processes; there is virtually no restriction on the range of business processes that can leverage its capabilities. The Cúram rules infrastructure is designed so that application logic is kept separate from rules processing. This helps reduce complexity and unnecessary rule executions. Cúram also ensures there is a clear separation between rules and the actual data or evidence that is evaluated by those rules, which allows the task of data maintenance to be considered separately from the management of rules.
5.4.4	Team NewWave designed the system architecture to decouple each layer of the system. This can be achieved by using load balancers and messaging middleware. Each layer, including the database, will have built-in redundancy to eliminate single points of failure. Such a design allows for high availability by automatically rerouting traffic to healthy nodes during a component failure. In addition, cloud services enable auto-scaling of components during traffic spikes. The architecture also includes active and passive failover support for DR using multi-region deployment. Team NewWave will deploy geo-redundant storage that automatically replicates to the alternate region, and the DB2 database synchronization capability supports having a copy of the database in the secondary (passive) environment. NewWave will deploy the system in MAG Arizona region as a primary site and Virginia as a secondary site. In the event of catastrophic failure within a region (e.g., due to a natural disaster), DNS failover is triggered, and the secondary environment becomes the primary (active), including replicated DB2 instance, and incoming traffic is routed over to the new active region. This mechanism supports rapid failover with limited service interruption.
5.4.5	The system is designed and implemented to gracefully handle exception conditions (e.g., data type mismatch). This is done primarily at the User Interface/User Experience (UI/UX) level by preventing the user from submitting data that are not correctly formatted. This can also be done at the system interface level by multiple levels of monitoring to ensure exceptions are reported back to the development team for triage and tracked. If the data received cannot be integrated into the system, the team will work with the data source partner to correct the data. System error conditions and non-recoverable events will be handled by automatic failover, as described in our response to SOW 5.4.4.
5.4.6	All system components will be deployed using Ansible, an open-source tool for Infrastructure as Code (also known as programmable infrastructure). Ansible supports various cloud platforms in public cloud, private cloud, and hybrid settings.
5.4.7	Team NewWave will work with both Arizona and Hawaii to gather detailed information such as number of users, expected growth rate, exact data mapping requirements, and number of environments with the type of expected data. This type of information is crucial to produce storage capacity estimates.
5.4.8	Following SOA principles and MITA guidelines, the proposed solution provides multiple ways to integrate with both internal and external systems using IBM Integration Bus (IIB). IIB is an implementation of ESB, an architectural pattern that supports abstraction and management of service interactions between entities. It is a flexible

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

	connectivity framework that promotes reliable and secure system integration between service providers and requesters, while reducing the number, size, and complexity of application interfaces.
5.4.9	Using ESB and a series of protocols—extensible Markup Language (XML); Simple Object Access Protocol (SOAP); Web Service Description Language (WSDL); and Universal Description, Discovery, and Integration (UDDI)—Team NewWave's solution architecture will support sophisticated data exchange and communications with other environments. For BPEL, IBM Cúram exposes WSDL for each workflow process web service that contains information that can be used by BPEL processes. User authentication and authorization is provided by IBM Security Access Manager (SAM) via Security Assertion Markup Language (SAML).
5.4.10	CMS expects the state to manage its own software development life cycle (SDLC), including conducting SDLC gate reviews, and the Medicaid Enterprise Certification Life Cycle (MECL) accommodates various approaches that states use to update or upgrade their Medicaid Management Information Systems (MMIS). Team NewWave selected the Scalable Agile Framework (SAFe) development approach. We will monitor changes to MITA checklist and artifacts requirements and will communicate each necessary change to respective stakeholders; modifications will be made during program increments. All modifications to the PMS will follow our AHCCCS/Med-QUEST approved change management process.
5.4.11	Using the IBM Integration Bus (IIB), data from multiple sources can be received via various protocols and data formats. IIB supports Simple Object Access Protocol (SOAP), Hypertext Transfer Protocol (HTTP), and Java Messaging Services (JMS) protocols and a wide variety of data formats, including standards-based formats (e.g., XML, Data Format Description Language (DFDL), and JavaScript Object Notation (JSON), industry formats (e.g., Health Level Seven International (HL7), American National Standards Institute Accredited Standards Committee electronic data interchange standard (X12), Electronic Data Interface (EDI), and Society For Worldwide Interbank Financial Telecommunication (SWIFT), and custom formats. NIEM Information Exchange Package Documentation (IEPD) is a collection of mutually supportive artifacts that define the content of a specific information exchange. It can be used in conjunction with WSDL to clearly and unambiguously specify a web services interface, including all the semantics. IIB can expose web services to be used for exchanging messages defined by NIEM IEPDs. Cúram supports the processing of data in multiple formats using its Application Development Environment (ADE). Please see Section A.24 for a detailed description of the ADE. Using its robust integration capabilities, Cúram can accept and produce data in standard XML as well as NIEM-formatted XML. It is more suitable to handle X12 at the ESB level.
5.4.12	Using ESB as SOA infrastructure and a series of protocols—eXtensible Markup Language (XML); Simple Object Access Protocol (SOAP); Web Service Description Language (WSDL); and Universal Description, Discovery, and Integration (UDDI)—Team NewWave's architecture will support sophisticated data exchange, integration, and communications with other environments.
5.4.13	Team NewWave follows a strict change control process and all changes and features added to our proposed solution will be transferred to AHCCCS/Med-QUEST. Our change control process falls under our Configuration Management Plan, as described in our PMP in Appendix B.
5.4.14	Team NewWave's solution has the capability, out-of-the-box (OOTB), to enable multiple forms of system- and business-level auditing, including the following: • Database Table Auditing • Business Function Auditing • Security Auditing (see SOW 5.15.1–10 and 5.16.10–11) • Workflow Activity Auditing. Team NewWave will provide training and configuration support for AHCCCS/Med-QUEST staff to generate ad hoc reporting requirements that may arise in the future.
5.4.15	See Section 5.4.4 for information about our rapid failover and redeployment in the event of planned or unplanned interruptions.

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

A.5 DETERMINE PROVIDER ELIGIBILITY (SOW 5.5)

SOW	Team NewWave Response
5.5.1	The solution contains configurable business rules within both the IBM Cúram Verifications engine and within the IBM Cúram Evidence Issues that can be used to prevent provider enrollment. Both items will provide the states with configurable options to either stop or allow enrollment based on data within the application, including data received from external interfaces or files from the provider.
5.5.2	During the application intake process, our solution searches submitted applications for duplicate providers, including in-progress, approved, and denied applications. If the search identifies a match, the system generates an issue, including an alert to a worker, on the application case that includes the findings and results of the other submitted applications. The providers on the new application are not enrolled until the issue is cleared by the user.
5.5.3	Team NewWave's solution allows a provider to enter multiple service locations. Once the provider is approved, these locations are stored within the solution on the provider's record. There is no upper limit on the number of service locations a provider can enroll.
5.5.4	The provider will have the ability, based on a configurable validation, to register multiple national provider identifiers (NPI). Multiple NPIs are stored on the provider's application and revalidation, if applicable, and stored on the provider's record once the applications are processed. Through a configurable option, the states can require the NPIs to be verified by the NPI registry before being stored on the provider's record permanently.
5.5.5	During the application process, the user is presented with an application that uses IBM Cúram's Intelligent Evidence Gathering (IEG) technology (a business service included in the Cúram Platform). IEG scripts can be configured from within the IBM Cúram Administration Application by authorized users. The IEG application script is configured with all information required for enrollment based on federal and state policies. The information collected through the enrollment process is mapped to the application, as shown in Appendix A, Figure 17, Application Evidence Dashboard. Once approved, the data are maintained on the provider's record within the solution.
5.5.6	The solution will determine each provider's eligibility using a defined workflow that performs a set of activities in accordance with state and federal policies. To begin, the system collects the enrollment application from the provider, or re-enrollment or revalidation information from an existing provider. During that process, the solution verifies new and existing provider data to confirm that all data are entered using the correct format or structure and that all required data have been entered during the application process. The application process can also include real-time license and database checks of provider information. During submission, the solution checks for duplicates and determines the outstanding items or documents that must be completed on the application. This information is stored on the application, as shown in Appendix A, Figure 18 Application Verifications. The provider's risk level is determined based on federal and state policies. Additional application information is verified with external entities, including NPI information, Medicare verification, and checks against exclusion and termination files as required by the state. The provider's application fee is determined as well, based on CMS policies. The provider has the opportunity to submit additional information, pay application fees, and sign agreement forms from their secure account as necessary.
5.5.7	Data retrieved from a variety of formats from licensing and certification interfaces are transformed and stored as non-editable (view-only) dynamic evidence, or data, on the application. The specific data types on the evidence can be defined and configured by the administrator for each type of evidence. These data can be used by any part of the system, including business and eligibility rules, validations, and reporting.
5.5.8	When determining provider eligibility, an automated workflow is used to ensure each step of the eligibility process is followed. During the application intake, verification interface calls are made to all applicable external interfaces and data are checked against exclusion lists and other types of state and federal provider data. If verifications are not met or if provider data is found that impedes the enrollment process, the provider application is pended according to state policies. For ongoing monitoring, the solution periodically reverifies provider enrollment eligibility from all applicable sources according to state policies. A workflow is used to notify the appropriate parties when a problem is found and to act in accordance with state procedures. The workflow can be configured to automatically dis-enroll the provider or generate a task to a worker to manually review the issue before dis-enrollment. Once a provider is dis-enrolled, a

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

	notification to the provider is generated.
5.5.9	The ability to perform real-time verifications, including license and certification checks from external entities, is included in the solution. Depending on the state's requirements, these real-time database checks can be made by using a call-out during the provider application process, which can notify the provider in real time of license issues, providing them with the opportunity to correct any data-entry problems. Real-time interfaces can also be called during the application intake process on submission and create an issue on the application in the event a license cannot be verified.
5.5.10	A pre-check search feature is available for internal workers. The pre-check search performs a name search against a catalog of data stored from a variety of sources, as determined by the state. The search looks for affiliates, group billers, subcontractors, and other providers and related participants in the system. Stored data include, but are not limited to, exclusion and termination files, criminal information, and bankruptcy information. Search results display information about the known providers and/or associated individuals, any available exclusion or termination match, criminal or bankruptcy information, and a list of known NPIs associated with the name.
5.5.11	Our solution allows the states to control the application process through a configurable workflow. The configured solution requires human review of the application before approval. When there are outstanding items and issues found on the application, they are clearly visible to the user on the application home page.
5.5.12	Using the IBM Cúram Priority, Complexity, and Risk (PCR) assessment tool provided in the solution, business rules can be configured to rate the priority of each application. These are configured for the states based on provider type.
5.5.13	The solution interfaces with the state's managed-care organization (MCO) credentialing system to receive provider credentialing information. The bi-directional interface can be either real-time or batch, depending on the technology supported by the current MCO credentialing system. The data received are stored on the provider's record within the Cúram Provider Management (CPM) system. In addition, the bi-directional interface will expose data known about the provider to the MCOs as required.
5.5.14	Risk levels are determined by the IBM Cúram PCR tool. Rules are configured based on CMS policy to determine the provider's risk. The risk level is clearly viewable on the provider's application, as shown in Appendix A, Figure 19, Application ACA Screening.
5.5.15	Fingerprint and criminal background details are tracked in each enrollment, reenrollment, and revalidation application process. If the provider is determined as moderate or high risk, as determined and tracked by the PCR assessment tool, a workflow is enacted that sends notification to the provider informing them of the elevated status and describes the need for the fingerprint and criminal background checks.
5.5.16	The need for a site visit is tracked as part of the enrollment, reenrollment, and revalidation application process, and details of site visits are captured in the solution. On application or when a change is reported, the PCR assessment tool reviews provider details to determine if a site visit is required based on the provider type. If it is determined that a site visit is required, a workflow is configured to notify the provider of the site visit requirement.
5.5.17	Team NewWave's solution maintains details of site visits for each provider, as shown in Appendix A, Figure 20, Provider Site Visits. This functionality includes a user-customizable wizard that allows the user to document the site visit and include only the pertinent information related to the specific site visit. Users also have the ability to upload additional documents and attachments as required.
5.5.18	Geo-locations are retrieved from an external interface, such as Google geo-coding application programming interfaces (API). Using the geo-coded location, a scheduling tool enables reviewers to schedule provider site visits based on the location. Site visits are not scheduled for providers who are on the state's do not enroll list or who have open investigations.
5.5.19	To comply with Medicare and Medicaid provider matches, our solution interfaces with external applications identified by the state. Configurable business rules allow the state to stop the enrollment of a provider who is required, based on provider type, to be enrolled in Medicare. If a provider claims to be enrolled in Medicare, but is not found, an issue is created on the application.
5.5.20	The AHCCCS/Med-QUEST solution manages the ongoing provider record within the system. Details, including the

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

status, effective dates, and end reasons, are tracked within the provider's record for each provider type. Authorized users have the ability to modify provider types and to end or begin new provider types based on the configuration rules of each individual type.

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

A.6 Enroll Provider (SOW 5.6)

SOW	Team NewWave Response
5.6.1	The enrollment status on the provider record within the solution designates the provider's status according to the state's business rules. The provider's status is easily viewable on the provider's home page. A history of the provider's status is also available within the provider's record. Enrollment status designations are configurable.
5.6.2	Multiple payment modalities are supported by the solution. For real-time credit-card transactions, the provider is directed to the state's payment gateway with Bank of America once the application is completed. Once a credit-card transaction is completed, it is recorded on the provider's financials tab within the provider's record. In addition, checks that have been cashed are also recorded for Hawaii. A history of all payments, regardless of the payment type, for applications, re-enrollments, and revalidations will be available and tracked in the provider's record within the solution.
5.6.3	In accordance with ACA provider revalidation requirements, the provider's revalidation is scheduled either 3 or 5 years from the provider's enrollment date, depending on the provider type. A configurable workflow may include the following steps. Step 1: Before the provider's revalidation date, a workflow is enacted that first notifies the provider. An example of a provider notification is shown in Appendix A, Figure 21. Step 2: The workflow enters a wait period until a response is received or additional notifications are generated, depending on the state's requirements. Step 3: The workflow can again enter a wait period until the revalidation date or a revalidation is received from the provider. If no revalidation is received, the workflow can automatically dis-enroll the provider and send notifications to interested parties, including the provider.

A.7 Disenroll Provider (SOW 5.7)

SOW	Team NewWave Response
5.7.1	The solution manages and tracks all individual relationships to a provider. If individuals are found debarred, listed in registries, or do not meet other defined requirements, affiliated provider records are suspended according to the configured business rules. The business rules can be configured to immediately suspend the provider or require manual action by a worker. Business rules also can be configured to check for restricted individuals during the application intake process. If the provider is affiliated with a restricted individual, the application can be automatically denied or require manual approval based on the configuration.

A.8 Inquire Provider Information (SOW 5.8)

SOW	Team NewWave Response
5.8.1	Team NewWave's solution includes comprehensive search functionality for both providers and applications. This functionality includes the ability to further filter results based on specific criteria, including reference numbers, date ranges, partial names, and status. The search result screen allows the user to sort each result set by any column included in the results. For example, when searching for an application, this functionality allows users to sort by provider, reference number, date, or status.
5.8.2	Applications are timestamped at various stages, including when they are initiated and when they are submitted. The applications are also associated with the provider record. The provider search functionality enables internal users to search for providers and the applications that were initiated or submitted by the providers. This search feature assists staff in answering a provider's questions about their applications. Documents uploaded by the provider are also timestamped, thereby giving state staff a complete picture of the provider's application and status.
5.8.3	The provider search included in the solution allows users to search for providers by licensure. The drop-down menu containing the licensure types is stored in a configurable code table.

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

A.9 MANAGE PROVIDER INFORMATION (SOW 5.9)

SOW	Team NewWave Response
5.9.1	The AHCCCS solution's portal allows providers to submit corrections to applications previously submitted from their online account. The provider is presented with a pre-populated summary page containing the provider's previously submitted application data. The provider can make updates by using links (edit, add, delete) adjacent to each section of information. Once the updates are completed, the provider submits the changes, and the changes are mapped to the related application case. New updates are shown as "In-Edit" evidence on the application case and can be reviewed and accepted by workers as required.
5.9.2	The solution stores effective start and end dates for each service type. A complete history, including effective dates for each service type, is maintained on the provider's record, as shown in Appendix A, Figure 22, Provider Types. The service start date is set to the date the provider screening is completed. Authorized users have the ability to override this date as required.
5.9.3	Team NewWave's solution is capable of document conversion and ongoing information transfers between AHCCCS/ Med-QUEST and any other information provider. The system can use existing APIs or other EFT processes for date transfers (see SOW 5.4.12 and 5.4.15).
5.9.4	The solution's portal allows providers to make updates to profile information. Each state determines which fields can be updated by providers, without the need for a new enrollment. The provider makes changes with a simple process, and views the current information, edits the existing information to be updated, confirms the updates, and then submits the profile change to the agency.
5.9.5	On exclusion of a provider, a written notification is sent to both the provider and CMS. A PDF version of both notices is stored on the provider's record. The template for this notification is configurable in the administration module.
5.9.6	Newly scanned images and documents are uploaded into the Open Source Alfresco Enterprise Content Management (ECM) solution. Alfresco supports an open standard known as Content Management Interoperability Services (CMIS). CMIS enables seamless integration between the PMS and Alfresco. Any existing documents that must be accessed through the proposed solution can be migrated if required. Once uploaded to the ECM solution, a corresponding attachment record is stored on the PMS, where the user is able to write notes and comments regarding the uploaded document. Annotations can be created on the document using popular desktop applications. For example, Adobe Acrobat allows PDF documents to be highlighted and contain embedded comments.
5.9.7	The document upload functionality within the solution's portal provides a tracking number for each upload submitted. After the upload is completed, the provider is shown the tracking number for the request. The tracking number can be used by internal users to search for documents that have been uploaded. Users can enter the tracking number in a document upload search screen and will be presented with the matching document.
5.9.8	The solution identifies providers who have been previously matched on the death, criminal, and excluded provider lists. Details, including the date, source, and reason, are available on the provider record. Providers found on criminal and excluded lists are not allowed to reenroll until the minimum time frame has expired. As new death, criminal, and exclusion files are processed, only currently enrolled providers are reported. A workflow notifies the appropriate party of the newly found match and business rules are configured to automatically suspend or terminate the provider or allow a user to investigate the match and take the appropriate action manually.
5.9.9	The solution's platform maintains a transaction log with auto-generated comments of any actions executed by the system or by users on an application or provider record. The comment includes a timestamp, a brief statement of the action taken, and the identity of the user, or system, that executed the action. The transactions on an application are available to view, as shown in Appendix A, Figure 23, Application Home Page.
5.9.10	In our solution the IBM Cúram Evidence Issue functionality lets users configure business rules in accordance with state policy, and lets users check for specific data conditions, deficiencies, or conflicts from external sources. Administrators can configure business rules for each evidence issue. When evidence is added, updated, or deleted, the evidence business rules are re-executed to check for data accuracy and completeness. The evidence issues give

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

	the user a clear list of the open issues on the evidence, and a link to directly correct the issue.
5.9.11	Tribal identifications are captured on the provider application and recorded on the provider record once the application is approved. The tribal details identify both non-IHS/638 and (Hospital Information System) HIS providers.
5.9.12	Team NewWave's Solution maintains complete details of the providers registered within the system. Each provider record contains a list of the providers contracted MCOs. This information is made available to the reporting solution, which enables users to identify each provider that is contracted by an MCO.

A.10 Manage Provider Communication (SOW 5.10)

SOW	Team NewWave Response
5.10.1	Our solution has several built-in workflows to provide notifications to providers when updates are made or when registration or status information is updated. Each time a provider's enrollment status is changed, a notification is generated, which is configured based on the agency's notice templates. In addition, there are built-in workflows to generate notices on service approvals, site visits, and provider changes. The solution uses these workflows to generate the appropriate triggers based on the agency's requirements.
5.10.2	The solution supports both electronic and paper correspondence. Based on the notification type and purpose, either an electronic email message is sent to the provider notifying them of a secure message in their account, or a paper notice is mailed. Paper notices are stored in the provider records as PDF documents. These notices are also attached to the provider's secure portal inbox. A history of all correspondence is stored on the provider's record.
5.10.3	The workflow that is enacted during the application intake process determines the provider risk level and determines if a AHCCCS/Med-QUEST site visit is required. If a site visit is required, the workflow automatically generates a notification and creates a task allocated to the appropriate site visit work queue based on the provider's location.
5.10.4	The workflow enacted during the application intake process determines the provider risk level and decides if a site visit is required to complete enrollment, re-enrollment, or revalidation. If a site visit is required, the workflow automatically generates a notification to the provider alerting them that a site visit is required to complete their enrollment, re-enrollment, or revalidation.
5.10.5	The solution's portal allows providers to submit requests to the agency containing both text and attachments. On submission of the request, the provider is given a tracking number. A task is created and sent to a work queue to handle the incoming provider requests. On completion of the request, a notification is sent to the provider's account.
5.10.6	The solution includes notice triggers based on events that occur as part of the provider lifecycle. The solution also includes a notice generation framework that allows for configuration of each communication by using templates that can be configured and uploaded in the administration module. Each template contains pre-defined text and dynamic content that can be defined based on provider types or additional attributes of the provider. If different notifications are required based on provider type, the workflow that triggers the communication to the provider can be configured to generate different notifications based on provider type or other attributes of the provider.

A.11 Perform Provider Outreach (SOW 5.11)

SOW	Team NewWave Response
5.11.1	The solution provides an Outreach Campaign functionality to display messages on specific provider homepages based on a set of configurations. Outreach Campaign configurations allow administrators to define targeted campaigns that can be displayed in the provider's account. The campaigns are based on information that the agency knows about the provider. For example, if the agency needs to communicate with providers in a specific geographic region or of a specific provider type, a message can be configured that targets only that set of providers.
5.11.2	Modern-day electronic communication systems, such as Constant Contact, typically have a set of Representational State Transfer (REST) APIs that can be used for integration. For example, Constant Contact itself has many documented REST APIs to create, update, and list Contacts, Contact Lists, Email Campaigns, Bulk Activities, and many others. Using the solution platform's ADE (see Section A.25), project implementation staff can easily create a new service that invokes one or more of the documented REST APIs.

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

For example, it is possible to export a subset of provider member contact details as Contacts, so it can be used within Constant Contact to send mass emails. Conversely, the solution can retrieve a list of Contacts from Constant Contact to communicate to providers through the provider portal.

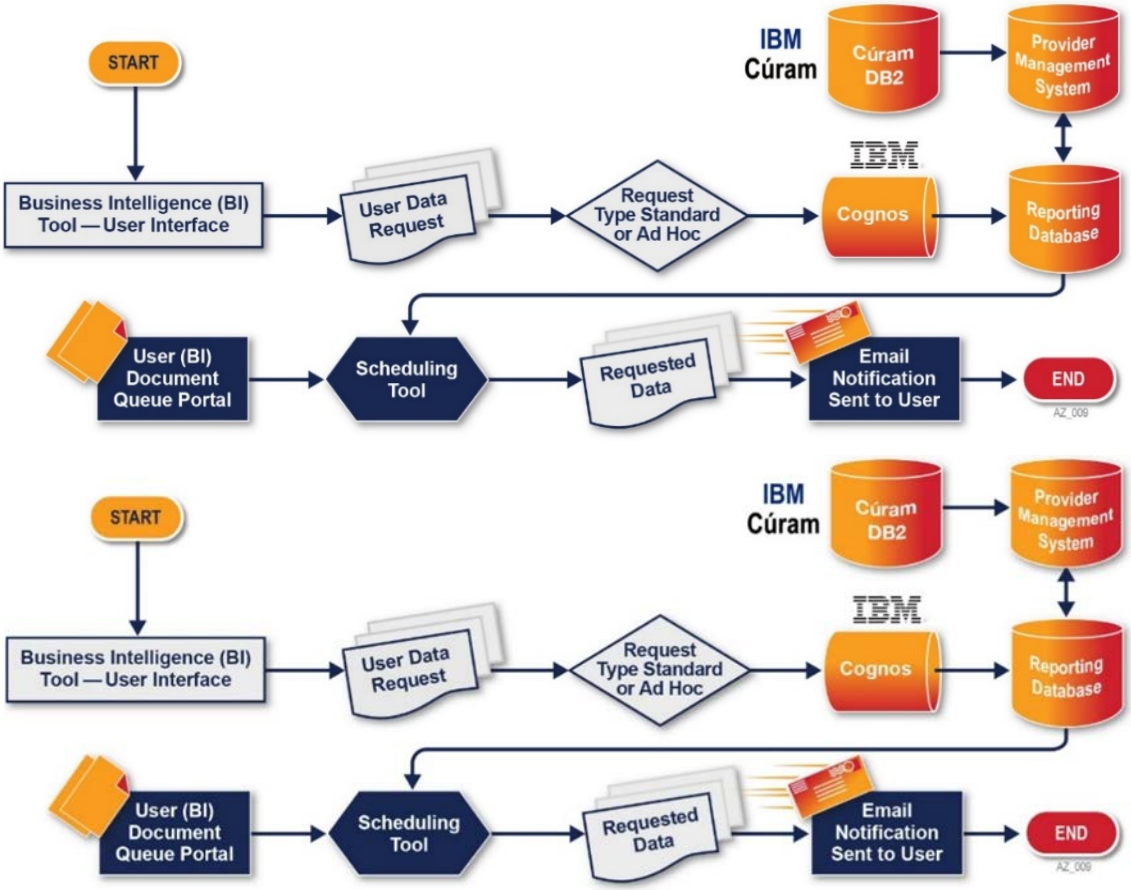
Team NewWave will work with the appropriate State staff to define the specific interface requirements.

A.12 Manage Provider Grievance (SOW 5.12)

SOW	Team NewWave Response
5.12.1	The Appeals feature in Team NewWave's solution provides comprehensive support for appeals processes by providing an integrated platform to document and manage appeals-related activities. It supports tracking and management of the appeal from the provider, documentation of details concerning the appeal, and the correspondence and workflow required to support these processes. This feature allows Arizona and Hawaii to deploy a flexible solution that supports the levels and types of appeals that are required by their specific appeals business process.

A.13 Reporting (SOW 5.13)

SOW	Team NewWave Response
5.13.1	Team NewWave's solution supports various reporting types and requests. Through batch control processing, the system delivers daily, weekly, and monthly reporting on all provider system activities. Alternative time frames may also be implemented, as agreed to by AHCCCS/Med-QUEST. In addition to periodic reporting, our reporting solution also meets ad hoc reporting needs. Figure 2 presents a high-level overview of the reporting process.



Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

	Figure 2: Reporting Process
5.13.2	The system provides access to pre-defined management dashboards to monitor enrollment application information in real time using IBM Cognos Business Intelligence (BI). The solution also provides dashboards and an OOTB library of standardized reports that can display data stored within the operational databases. If the data source being requested resides outside the operational databases, then Team NewWave will use the capabilities of Cognos to bring the data sources together for reporting. A wide array of reporting is available, including summary and detail-level reporting, as discussed in SOW 5.13.9.
5.13.3	Cognos Query Studio is the reporting tool for creating queries and reports in IBM Cognos BI, including ad hoc queries and reports. Users can create reports and view data in a simplified, drag-and-drop environment. Authorized users create new reports by opening existing reports, changing them, and saving them under a new name. While reports created in Query Studio can also be opened in Report Studio, most users prefer the simplified user interface offered by Query Studio for more professional formatting and conversion to templates. Cognos SQL supports current American National Standards Institute (ANSI) standards. Supported queries include left and right outer joins, unions, intersections, minus operations of multiple data sets, and multi-pass or correlated sub-queries. Query Studio also allows authorized users to view and modify the query details of a report, such as query parameters.
5.13.4	See SOW 5.13.3 for a description of Cognos Query Studio, which we use to support AHCCCS/Med-QUEST.
5.13.5	Cognos uses standard ANSI SQL to analyze and query data, which includes operators, wild cards, and Boolean expressions.
5.13.6	Our proposed solution uses both Cúram and Cognos BI to display reports in a variety of formats. The solution's web application displays embedded reports using an open-source technology—Business Intelligence and Reporting Tools (BIRT)—which allows for a variety of format displays, including charts and graphs. Cognos is used for robust standard and ad hoc analytical reporting and allows for a wide array of report formats without the need to export the data to another tool.
5.13.7	The proposed solution's operational database contains the source data elements related to the providers' records, including identifying information such as NPIs and other provider characteristics. This information can be presented in various formats, including on the application's web pages or as a report. If required, the data can be sent to the analytical data warehouse where Team NewWave will produce reports using the Cognos report design and generation tool.
5.13.8	Please see our response to SOW 5.13.1 and 5.13.3 for a detailed description of the Cognos BI and Cognos Query Studio, which we propose to use to support access to relevant data for authorized users.
5.13.9	The Cúram database is the source of detailed information regarding providers and their enrollment status. Team NewWave works with state staff to refine the specific requirements around the provider report capability and either provides the reports as part of our Cognos report catalog or as an embedded BIRT report from within the solution. For example, summary-level information can be generated in a Cognos dashboard report, whereas detail-level information can be a BIRT report within the PMS. Alternatively, this can be implemented as a drill-down report in Cognos, allowing for both summary-level and detailed-level reporting.
5.13.10	Errors that are logged in the system can be analyzed and reported on by Splunk, an operational intelligence and log management tool used by enterprises for robust log analysis. Splunk provides monitoring, correlation, and troubleshooting across every layer of the stack with key performance indicators. It provides deep drill-downs, statistical analytics, and real-time dashboards. Splunk also correlates the error in the log with the provider's username that was used to log in to the system and provide a detailed report to interested parties.
5.13.11	Cognos BI supports creating of reports on-demand or on a schedule. A report can be scheduled to run on different frequencies and can be configured to be saved to a specific folder location so that it is accessible to all users with read permission on that folder. Scheduled reports can also be sent to an email distribution list. Emails can either contain a URL to view the reports online or the reports can be attached to the email.

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

5.13.12	The Cognos reporting solution allows authorized users to search for available reports using report names and descriptions. It also provides a capability to search on dependencies, such as included column and data elements. The search results can also be refined using various filters, such as report type, data, owner, and others.
5.13.13	Authorized users can apply a template to report pages and prompt pages to give them the same look. For example, an IBM Cognos Query Studio template can be used to customize page headers and footers and to re-style layout objects. By default, Query Studio uses a system-wide template. Team NewWave will work with Arizona and Hawaii to apply the appropriate header and footer styles for the project.
5.13.14	The database is maintained with the appropriate level of historical data, as determined by AHCCCS/Med-QUEST to meet the required reporting needs.
5.13.15	Team NewWave's solution has multiple tools to collect statistics and information on the system and its environment. The tools range from our built-in monitoring mechanism, JMX, for statistics on performance of a transaction within Cúram, to Splunk, which provides monitoring, correlation, and troubleshooting across every layer of the stack with key performance indicators. We monitor our solution's services and respond to anomalies and incidents as they occur on a severity-level basis (see our response to SOW 5.15.17). As a standard best practice, we also review daily, and weekly reports generated by our tools for trend analysis that indicate any capacity, responsiveness, or security issues (see Section A.26). These are consolidated into a report and submitted at least monthly to AHCCCS/Med-QUEST describing the anomalies and resources involved in the resolution.
5.13.16	Team NewWave uses Jira to track change requests from submission, approval, implementation, testing, into production. It allows status updates to be made for changes; attaching artifacts (e.g., test results); and producing reports on the progress of changes. Please see our response to SOW 5.18.3 for additional information on Jira.
5.13.17	We use Jira to track defects, bugs, and issues found in the testing and production environments. We ensure designated state staff have full visibility into system support activities. We assign severity levels to tickets for agreed-on SLAs.
5.13.18	Please see our response to SOW 5.13.3 for a description of the toolset used.
5.13.19	Team NewWave will work with AHCCCS/Med-QUEST to provide statistical and historical trending reports from the database using the suite of tools available from the Cognos BI suite. Using the reporting architecture shown in Figure 2 from SOW 5.13.1, 10 years of historical data will be stored (as per item 105 from the published Q&A document) and made available for reporting. Team NewWave has experience in managing robust analytical solutions such as the Chronic Conditions Warehouse (CCW). Our CCW team implemented sophisticated data migration and integration processes with new and external data sources. Team NewWave developed and maintained the current www.ccwdata.org website, which included data file documentation, user guides, program statistics, cohort estimation tools, and other resources.

A.14 Solution Help System (SOW 5.14)

SOW	Team NewWave Response
5.14.1	During the enrollment process, a provider steps through the provider enrollment script using Cúram's Intelligent Evidence Gathering (IEG) question and answer script technology. This technology can be configured with embedded help text and links to external resources such as websites, documents, and training modules, providing context-sensitive help. Because this feature is configurable, the links and the content can be configured by an application administrator and have it effective immediately in the system. Help links can also be embedded throughout other portions of the enrollment process; for example, there can be a header link that directs the provider to a FAQ page. Alternatively, because they are standard HTML links, they can direct the user to specific training modules.
5.14.2	For internal users, all pages can have embedded help text that is configured into properties files separate from the web page logic. This separation makes it possible to update the help content without affecting the web page logic and without extensive developer involvement. Each page with embedded help has a question mark icon on the top right, which, if clicked, opens in a new browser window and links to the page-specific help topic. The help content is formatted in standard HTML; therefore, it can be embedded with rich font and text and supporting

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

images to assist the user in understanding the business process.
For external users, see our description in response to SOW 5.14.1.

A.15 System Availability (SOW 5.15)

SOW	Team NewWave Response
5.15.1	Team NewWave will deploy New Relic, which is an industry-leading application monitoring tool. Monitoring dashboards and alerting are developed to ensure the environment is monitored 24x7. The performance monitoring dashboard will have an availability of 99%, 24x7.
5.15.2	Team NewWave will deploy the solution in a highly available configuration with an active data center in Arizona, where our monitoring tools will automatically failover the application to a passive data center in Virginia if the application is unresponsive. This ensures 99.5% uptime. NewWave will inform the state immediately if there are any availability issues. See our response to SOW 5.15.1 for information on the monitoring tool and dashboard.
5.15.3	Team NewWave's solution maintains in a retrievable format all revisions of documents unless they are removed. Even if removed, they are stored in a backup file that can be restored if needed. Daily incremental, weekly, and monthly full backups allow for retrieval of any data within 1 day. NewWave stores daily and weekly backups for 1 year. NewWave stores monthly backups until the end of the contract. Team NewWave uses IBM Optim Data Growth to archive application data from the PMS solution. It allows for a rules-based archival process, which is scheduled to minimize the impact on production users and in accordance with the state's availability requirements. Using Optim, database tables can be archived in their entirety or a subset can be archived; the same is true for retrieval of data. The business rules that Team NewWave implements ensure that the solution complies with the states' data retention and retrieval policies.
5.15.4	The IBM Optim Data Growth solution not only can archive data to an archive file, but also can purge history data from those archived files. The solution can be configured to purge historical data according to the state's defined business rules. Team NewWave also ensures the process is non-disruptive to production users and in accordance with the state's availability requirements.
5.15.5	If production data are purged, Optim can restore the data from the archive file back into the production database. According to the database incremental backup schedule (see SOW 5.15.3), that mechanism can also be used to restore data. Team NewWave ensures the restore process is non-disruptive to production users and in accordance with the state's availability regulations.
5.15.6	NewWave uses NewRelic to monitor storage and system performance, by testing average response times and reads and writes to the database. NewWave uses the data to optimize and correct storage issues. See our response to SOW 5.15.1 about our performance monitoring dashboard.
5.15.7	Team NewWave ensure all data received from real-time interfaces are processed and accessible within 3 seconds of receipt. NewWave also works with interface sources to move to real-time data streaming where possible, making data available faster than batch processing allows. NewWave uses ESB along with NewRelic to ensure data processing does not violate SLAs. Our solution is built to respond to load, and NewWave will size the infrastructure to process the data in line with the SLA.
5.15.8	The data infrastructure deployed is highly available and scalable. In this way, the DB2 cluster automatically increases the number of nodes depending on the number of transactions per second. NewWave uses our monitoring tools to ensure that queries do not take more than 3 seconds to output results and that complex queries of more than 10,000 rows do not take more than 30 seconds.
5.15.9	NewWave ensures that discrete transactions do not exceed 2 seconds for response time. NewWave deploys monitoring tools that automatically test response times of various modules within the system. NewRelic has the capability to load user interfaces from different locations in the United States and to test response times as if it was a user. NewWave use these data to optimize the solution and limit latency.

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

5.15.10	NewWave ensures that adding, updating, or deleting data from operational components does not exceed 3 seconds. We use NewRelic to test adding, updating, and deleting of test data on non-production schemas within the DB2 cluster to ensure the SLA is not violated. NewWave uses these data to optimize the system and to take corrective actions if necessary. See SOW 5.15.9.
5.15.11	See SOW 5.15.1–5.15.10 about our performance monitoring dashboard.
5.15.12	Team NewWave develops detailed disaster recovery documentation and conducts business continuity testing. Our solution will be recoverable in 4 hours in the event of unscheduled downtime. See SOW 5.15.1 about our performance monitoring dashboard.
5.15.13	NewWave ensures continuity of services in the event of an interruption by implementing our Organization Business Continuity (BCON) Plan. See Section 6.1.19 of our Project Management Plan (PMP) in Appendix B.
5.15.14	Team NewWave monitoring includes conducting failover and disaster recovery testing before going live, conducting annual tests, and providing the results to AHCCCS/Med-QUEST within 30 days of completion.
5.15.17.1	Team NewWave agrees to abide by the time frame for Priority 0 Errors (system unavailable).
5.15.17.2	Team NewWave agrees to abide by the time frame for Priority 1 Errors (serious production issues).
5.15.17.3	Team NewWave agrees to abide by the time frame for Priority 2 Errors (significant production issue where work around is available).
5.15.17.4	Team NewWave agrees to abide by the time frame for Priority 3 Errors (all others).
5.15.17.5	Team NewWave agrees that all priority levels shall be subject to AHCCCS/Med-QUEST review and approval.
5.15.17.6	Team NewWave will work with AHCCCS/Med-QUEST to receive and provide contact information for reporting incidents in SOW 5.15.17.
5.15.17.7	Team NewWave will provide an acceptable risk mitigation plan within 5 business days of risk identification for 100% of high or critical risks.
5.15.18	Our proposed solution leverages IBM Integration Bus (IIB) to provide data exchange interfaces for the state's internal and external data exchange partners. IIB is an implementation of ESB, a SOA pattern. IIB synchronizes data across internal and external processes, and all interfaces are managed and orchestrated by IIB.

A.16 SECURITY (SOW 5.16)

SOW	Team NewWave Response
5.16.1	Team NewWave will ensure that all infrastructure meets Arizona Security Controls 2017 and will provide real-time compliance and vulnerability monitoring. We will schedule remediation according to the security policy and change control policy as agreed to with the agency.
5.16.2	NewWave will deploy Splunk, an advanced log aggregation and monitoring tool, and will configure it to use machine learning to identify usage anomalies, which can consist of a single action or a series of actions. A NewWave security analyst will review the logs and report any incidents of misuse to AHCCCS/Med-QUEST. Detailed usage reports can also be generated by Cognos; they can be created ad hoc and provide detailed reports of user activity within the system.
5.16.3	We use Splunk to maintain logs of all actions taken by system users and maintain them for the life of the contract. Reports of any actions taken by users can be produced as required. The solution also keeps a database log of a user's authenticated access to the system as well as unauthorized attempts to access information within the application. These database tables can be queried and reported to the appropriate staff. System changes also are by an audit feature within the solution, which can be turned on for certain database tables. Once turned on, changes made to data are captured along with a timestamp and the username of the user

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

	initiating the change. Please see our response to SOW 5.16.11.16 for more information on auditing.
5.16.4	All data are encrypted at rest on the physical hardware. This is accomplished using Azure Key Vault, which uses Data Encryption Key and Key Encryption Key, along with Azure Active Directory, to allow applications to decrypt data at rest only after the user's credentials are verified. DB2 databases that contain PHI and PII are encrypted at the software layer.
5.16.5	NewWave provides an independent third-party to perform penetration and security testing, within 6 months before implementation and annually. We provide the results, along with mitigation plans for any findings, to AHCCCS/Med-QUEST.
5.16.6	All Team NewWave staff with access to data are required to sign confidentiality agreements and return them to AHCCCS/Med-QUEST. Team members also are required to attend privacy and security training once per quarter. NewWave deploys advanced monitoring and security tools, including Splunk, Nessus, and Next Generation Firewalls, which together along with Microsoft Azure Cloud platform ensure that all AHCCCS/Med-QUEST data are protected.
5.16.7	All systems display a security banner with either the National Institute of Standards and Technology (NIST) compliant wording or other wording the state requires.
5.16.8	Team NewWave ensures that critical vulnerabilities are patched within 3 business days and that major vulnerabilities are patched within 10 business days. Team NewWave ensures this is completed by continually monitoring the environment and planning patches via a detailed change control process. See Section A.29.
5.16.9	All user accounts are individual and unique (shared accounts are disallowed). NewWave uses multiple data points to identify users and usage, which includes email, name, address, and phone number. These criteria are also used to see if a provider already exists. This process helps prevent the creation of duplicate accounts. Account activity reports are reviewed weekly as an additional means to prevent or act on duplicate accounts. All account activity is monitored by the security team—human read, not automated.
5.16.10	Team NewWave provides a written report, prepared by our security team within 12 hours of any security incident, that includes details of the type, scope, and impact of the incident along with any actions already taken or planned.
5.16.11	Team NewWave will comply with all laws, regulations, and standards listed in SOW 5.16.11.1–5.16.11.21. We inform AHCCCS/Med-QUEST where there is a conflict in law, regulation, or standards and use our risk and change management process to ensure we remain in compliance with state requirements. Our proposed solution has a built-in OOTB mechanism to support both authentication and authorization for application security. The built-in authentication can be turned off in favor of a configurable integration with a lightweight directory access protocol (LDAP) 3.0 directory for user authentication. Team NewWave ensures the authentication of users meets agency requirements. Our proposed solution also offers a robust and configurable role-based access control (RBAC) mechanism. Once authenticated, the application enforces user authorization using assigned roles and function and data identifiers. Each role is afforded specific permissions and denied all others. For example, a facility manager user who works on provider data, enters facility information, and so on, but who does not need to work on any financial aspects, does not have access to financial information; that is, the role is configured to exactly meet the user's needs. The agency, with Team NewWave's guidance, can define all the security roles it needs. Once configured, users are permitted to access only those functions and data that are explicitly authorized for that role. View-only roles are also configurable. Our proposed solution has the capability, OOTB, to enable multiple forms of system- and business-level auditing, including the following: • Database Table Auditing • Business Function Auditing • Security Auditing (see response to SOW 5.16.10 and 5.15.1–10) • Workflow Activity Auditing. Database auditing allows the system to capture actions carried out on the information held in the solution database

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

	tables, including the user ID, table name, date and time, and other pertinent information. Security auditing allows the system to capture authentication attempts as well as authorization failures. All auditing information is stored in database tables and can be easily extracted for reporting purposes.
5.16.11.1	Team NewWave complies with HIPAA Privacy and Security, specifically, CFR Title 45 Public Welfare, Part 164–Security and Privacy.
5.16.11.2	Team NewWave complies with AHCCCS/Med-QUEST security standards and policies set by Arizona Department of Administration (ADOA) and Arizona Strategic Enterprise Technology (ASET).
5.16.11.3	Team NewWave complies with NIST Special Publication 800-30 Revision 1 guidance for conducting risk assessments of federal information systems.
5.16.11.4	Team NewWave complies with Seven Standards and Conditions (CMS).
5.16.11.5	Team NewWave complies with all applicable ACA requirements and standards.
5.16.11.6	Team NewWave works with an independent, third-party contractor to conduct an Annual Security and SSAE 16 Assessment or equivalent. The annual security assessment covers vulnerability testing, penetration testing, and process and procedures related to the systems.
5.16.11.7	Team NewWave resolves high and medium vulnerabilities identified and discusses low vulnerabilities before resolution. Based on feedback from AHCCCS/Med-QUEST, we will remediate identified issues.
5.16.11.8	Team NewWave provides Security Incident Reporting.
5.16.11.9	Team NewWave monitors emerging information security threats and vulnerabilities and the necessary remediations.
5.16.11.10	Team NewWave works with AHCCCS/Med-QUEST and provides system documentation, onsite training and training manuals, and desk-level procedures and practices to avoid security breaches.
5.16.11.11	Team NewWave uses LDAP version 3.0 or higher to manage user authentication and authorization.
5.16.11.12	Our solution contains verification mechanisms that are capable of authenticating authority (as well as identify) for the use or disclosure requested.
5.16.11.13	The proposed solution enforces an RBAC model for authorized access. This model, when applied to individual data fields on a user screen, automatically checks the logged-in user's security role against the data elements on the screen. If the user does not have the assigned security identifiers, the screen displays a set of asterisks (*) instead of the real data value. This effectively prevents unauthorized access to records.
5.16.11.14	To ensure security, we enforce password policies based on length, character requirements, forced reset intervals, and updates, as defined by AHCCCS/Med-QUEST.
5.16.11.15	To ensure security, our solution has the capability for expiring or terminating a user's session after a predefined period of inactivity.
5.16.11.16	Our solution can audit and track all activity, by user and process, including date and time of last login, invalid login attempts, system errors, and transaction activities, including inquiries. We alert appropriate staff of potential violations, including inappropriate access to confidential information. We preserve audit data when security violations are detected.
5.16.11.17	Our solution enables us to redact records, in whole or in part, according to state and federal privacy standards based on role and authority.
5.16.11.18	As requested, we provide AHCCCS/Med-QUEST with access to source code, libraries, and other project artifacts.

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

5.16.11.19	For security, we initiate corrective actions to ensure a breach does not occur again, if it is within our scope of responsibility. We prepare and retain documentation of breach investigations and provide copies within 24 hours of detection of the breach.
5.16.11.20	We prevent the installation or use of remote control or file sharing software unless explicitly approved by the state.
5.16.11.21	As mentioned in SOW 5.16.11, we adhere to applicable state and federal laws, rules, regulations, guidelines, policies, and procedures related to information systems, information systems security and privacy, physical security, and PHI confidentiality and privacy. We will work with AHCCCS/Med-QUEST to define and determine if the proposed systems or services meet applicable compliance requirements. If there are issues, we will develop a mitigation plan within 10 business days to regain compliance with mitigation and testing.
5.16.12	All NewWave staff take annual HIPAA security training; we will provide proof of completion for each staff member on request.

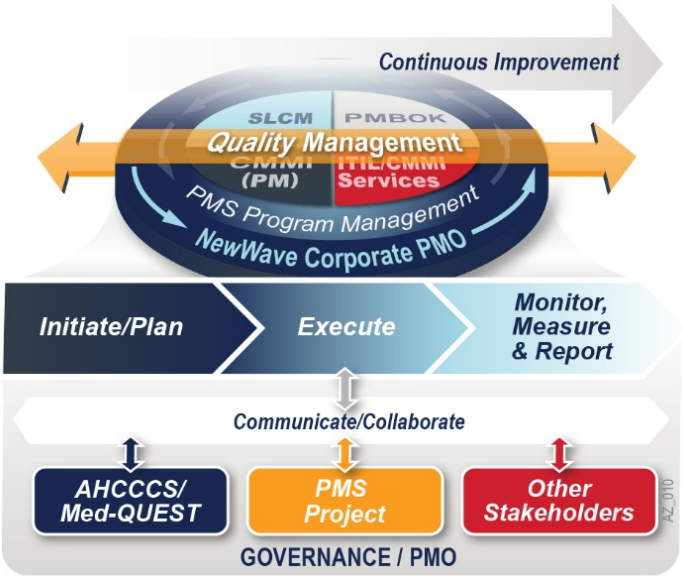
A.17 Project Governance (SOW 5.17)

SOW	Team NewWave Response
5.17.1	Team NewWave meets the MECL and IV&V requirements as described below and in Section A.27.
5.17.1.1	Team NewWave supports AHCCCS and Med-QUEST and authorized contractors in the IV&V process. We understand that the state's expectations may include document creation, information requests, and other support activities for the IV&V process. We ensure that IV&V support tasks are tracked in our Project Work Plan.
5.17.1.2	Team NewWave ensures our Change Management Plan, referenced in our PMP, is consistent and aligned with the AHCCCS/Med-QUEST Enterprise Change Management Plan.
5.17.1.3	Team NewWave will coordinate with AHCCCS/Med-QUEST and the IV&V Contractor to align our Project Work Plan tasks and schedule with the Integrated Master Plan. We work collaboratively to communicate risks and issues that might affect our schedules to ensure AHCCCS/Med-QUEST will meet all CMS requirements.
5.17.1.4	Team NewWave dedicates resources from the beginning of our implementation planning to ensure compliance with all MECL requirements.
5.17.2	Team NewWave will support AHCCCS/Med-QUEST in all program governance activities and provide all required information for the state to complete its State Self-Assessment (SS-A) for the Medicaid Information Technology Architecture (MITA) initiative. We have experience helping states meet MITA requirements and CMS governance through our MACBIS and T-MSIS contracts with CMS. As the Medicaid and CHIP Business Information Solutions System Integrator (MACBIS SI) for CMCS, NewWave is responsible for governance across the MACBIS enterprise, including making recommendations for improvement, training, and implementing processes and tools for data, security, system, infrastructure, and business governance.

A.18 Project Management (SOW 5.18)

Team NewWave understands the importance of providing the States of Arizona and Hawaii with a Provider Management System (PMS) that is delivered seamlessly, on time, and with a high level of quality. Our team's experience in executing project management, systems integration, and development processes and methodologies provides the states with a high level of confidence in our ability to meet the PMS contract requirements. Team NewWave will leverage our CMMI-appraised (Level 3 for Development; Level 4 for Services), International Organization for Standardization (ISO) 9001 processes, including our agile project management practices, which align with the Project Management Institute's Project Management Body of Knowledge® (PMBOK®), and the Scaled Agile Framework (SAFe). Our approach deploys the right people, processes, and technology on contract award, and we will tailor our management framework to meet the specific needs of AHCCCS/Med-QUEST, while providing visibility into current progress and the flexibility to meet future requirements. The PMP and Project Work Plan presented in Appendix B and Section A.18.b, respectively, represent the processes and methodologies we leverage to ensure project success.

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.



In determining our COTS solution to meet the AHCCCS/Med-QUEST vision and requirements, NewWave considered several of our strategic product partners. Based on our evaluation and experience working with IBM in the past, we concluded that IBM's Cúram Social Program Management Platform (SPMP) is the best fit for implementing the new Provider Management System (PMS). IBM is the market-leading health and human services COTS platform and we have worked with IBM to implement Watson Health's cognitive capabilities into CMS' physician quality help desk.

As described in our PMP, Team NewWave uses sound program and project management practices, while leveraging our agile practices to drive transparency and customer involvement across the implementation and operations phases. Our management framework monitors and controls the overall project, while ensuring the product meets stakeholder needs throughout implementation into operations. Our proactive risk management process (described in our PMP) mitigates risk and ensures stakeholder awareness in meeting their requirements.

Team NewWave provides overall project oversight to ensure delivery of all activities within defined timelines. The program management team manages all required staffing, status reporting, enterprise scheduling, risk management, change management, and communications. The project management team also ensures consistent use of tools, while tracking and reporting on all performance measurements.

Figure 3: Team NewWave's PMO Approach

SOW	Team NewWave Response
5.18.1	NewWave ensures continuity of services in the event of an interruption by implementing our Organization Business Continuity (BCON) Plan. See Section 6.1.19 of our Project Management Plan (PMP) in Appendix B.
5.18.2	Team NewWave monitoring includes conducting failover and disaster recovery testing before going live, conducting annual tests, and providing the results to AHCCCS/Med-QUEST within 30 days of completion.
5.18.4	Team NewWave's Project Manager will tailor our standard Responsible, Accountable, Consulted and Informed (RACI) process and template to match the AHCCCS/Med-QUEST RASIC matrix. Our proposed RASIC is included in the Communication Management Plan of our PMP. In accordance with the AHCCCS/Med-QUEST RASIC matrix, Team NewWave's Communication Plan defines meeting types, purposes, frequency, audience, and logistics (i.e., meeting location or dial-in information for virtual participation). Using defined templates, we prepare meeting agendas for the state no later than 1 business day before the respective meeting. We document and prepare meeting minutes and distribute them to the state no later than 2 business days after the meeting. Minutes include action items, decisions, program risks, and issues. All meeting materials are stored in the PMS Project Management Portal.
5.18.5	The Project Work Plan (PWP) defines the activities and deliverables necessary to meet SOW requirements. All deliverables are placed under configuration control and are identified in the Configuration Items list of the Configuration Management Plan. We track and access item delivery via the PMS Project Management Portal. The portal in SharePoint provides access to all PMS documentation, deliverables, dashboards, and reports, and promotes collaboration among Team NewWave, AHCCCS/Med-QUEST, and other stakeholders.

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

	We will use AHCCCS/Med-QUEST libraries of document templates if required or leverage our CMMI Level 4–appraised and ISO 9001:2015–approved library of templates and processes. These templates will serve as a foundation for the state's approval and for planning and documenting the work. Each project deliverable will be delivered to the state in a media, format, and time frame as required. To ensure timely delivery, we discuss upcoming deliverables at weekly internal meetings and on the project dashboard. Deliverable review and acceptance is discussed in SOW 5.18.10.1-5.18.10-4.
5.18.6	On contract award, Team NewWave's Communication Plan will define meetings and reporting, including status reports and status meetings. Deliverables, milestones, issues, risks, and SLAs will be available for status review via dashboards. All recurring meetings and deliverables will be included in the PWP approved by the state. All meetings will include a combination of onsite and remote NewWave staff.
5.18.7	Team NewWave will facilitate meetings with the state and other stakeholders. Formal and frequent project meetings provide stakeholders with consistency, clarity, and expectations.
5.18.8	Team NewWave will use our standard project meeting agenda template, tailored to the needs of the state. The agenda typically includes risks, issues, action items, progress, resource and system changes, and SLAs when appropriate.
5.18.9	NewWave uses SharePoint for our electronic document repository on all current contracts. However, if AHCCCS/Med-QUEST requires a different tool, we will tailor our processes to work with the required tool.
5.18.10	All deliverables are defined in the PWP. We will tailor our process and timelines to meet the needs of the AHCCCS/Med-QUEST team.
5.18.10.1	Activities will be scheduled for Team NewWave internal reviews and the delivery of drafts to the state, as well as time for the state to review and provide comments, and for Team NewWave to revise and resubmit. Major deliverables may also include scheduled walkthroughs. Team NewWave normally allocates a total of 8 business days for approval of the final deliverable: 5 business days for state review and comments; 2 business days for NewWave to respond to comments; and 1 business day for final approval. This timeline can be extended for complex and extensive deliverables.
5.18.10.2	Our technical leads develop deliverables, our project coordinator tracks timelines, and our project manager has final approval and sign-off responsibility for all deliverables.
5.18.10.3	NewWave will implement our CMMI and ISO-certified peer review process for all deliverables to AHCCCS/Med-QUEST. Our QMO performs a quality check monthly on the results and quality of these reviews. The project manager is responsible for ensuring our peer review processes are followed.
5.18.10.4	Team NewWave, in coordination with AHCCCS/Med-QUEST, will review and update our PWP schedule as needed to ensure multiple deliverables are not provided simultaneously.
5.18.11	As part of NewWave's standard practices, we conduct peer reviews on all contract deliverables. Peer reviews and deliverables are monitored by the NewWave corporate QMO and the corporate PMO. Based on feedback from the state's review, NewWave updates our peer review standards to improve the quality of future deliverables.
5.18.11.1	The peers in our internal review process have responsibility for reviewing all deliverables for accuracy, content, and scope. Metrics are collected and reviewed for the number of defects and changes required for trend analysis and to drive improvements in our review process.
5.18.11.2	Our writers and peer reviewers review the level of technical details and clarity of each deliverable. Our project manager also reviews them for appropriateness to the audience.

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

5.18.11.3	Our technical writer ensures proper English is applied and that each document is clearly understood. Every deliverable falls under our Configuration Management change control process.
5.18.11.4	In our peer review process, each reviewer checks for correctness of diagrams, graphs, and tables used in a deliverable. Our technical writer also reviews for clarity and readability.
5.18.11.5	Team NewWave follows industry standards and best practices to generate content and formatting reports and deliverables.
5.18.11.6	Our technical writer's review includes ensuring that references are verified and readily available for AHCCCS/Med-QUEST use.
5.18.12	Our Project Management Plan (PMP), including the PWPs, describes our mature, repeatable program and project management processes in detail. It describes how we initiate, plan, control, and track contract activities, so all deliverables, artifacts, and reviews are consistent and compliant with state requirements and NewWave's best practices. The PMP includes subsidiary plans, such as the Risk and Issue Management, Communication Management, Financial Management, Change Management, Configuration Management, Quality Management, Staffing/Resource Management, Schedule Management, and Development Approach. Our PMP, PWP, and schedule drive all successful program execution. Refer to Appendix B for the draft PMP.
5.18.13	Team NewWave manages all project activities in the PWP. Using agile methods, we measure progress based on sprint completion (backlog items completed and acceptance by stakeholder) and ensure strict adherence to the PMS solution release schedule. Refer to Section A.18.b for PWP timeline.
5.18.14	Module deliverable and milestone walkthroughs are coordinated with AHCCCS/Med-QUEST and scheduled in the PWP. Team NewWave proposes to implement capabilities following an agile methodology using sprints whereby we work with the state to timebox and prioritize user stories into features and epics. At the end of each sprint (every 2 to 4 weeks) there is a sprint review with the product owner and stakeholders (i.e., a walkthrough). This review demonstrates a set of capabilities as prioritized before each sprint begins. After an agreed number of sprints, we conduct a Business Playback session to stakeholders demonstrating a major component of the Provider Management System (an Epic). See our PMP's Deployment Plan in Appendix B for details.
5.18.15	As part of Team NewWave's financial reporting, we provide a report based on data from our Joint Application Management Information System (JAMIS) accounting system and Jira, which details tickets invoiced to the hourly pool, including hours used and hours remaining.
5.18.16	Team NewWave's culture and expectation is to operate as a partner with AHCCCS/Med-QUEST with a shared goal of implementing a solution that meets all expectations. This partnership requires us to act with transparency and openness, proactively identifying and mitigating risks to the project, communicating openly and frequently with stakeholders, and being good stewards of the resources entrusted to Team NewWave. We will provide data-driven status reports through online dashboards that can be tailored to meet AHCCCS/Med-QUEST information needs.
5.18.17	Team NewWave uses SharePoint online and Jira as our collaboration site to include technical and non-technical artifacts. All development artifacts, such as requirements, user stories, storyboards, Software Design Description (SDDs), supplemental specifications, test cases, scripts, and results, and user and system documentation are stored and accessible to stakeholders based on user permissions. If AHCCCS/Med-QUEST prefers a separate site, we will ensure that all artifacts are maintained on the required site.
5.18.18	All system and services documentation is placed under configuration control and identified in the Configuration Items list in the Configuration Management Plan. We track and access item delivery via the PMS Project

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

	Management Portal. The portal provides stakeholder with access to all PMS documentation, deliverables, dashboards, and reports, and promotes collaboration among Team NewWave, AHCCCS/Med-QUEST, and other stakeholders. This documentation also can be directly transferred to AHCCCS/Med-QUEST if required.
5.18.19	In the event of transition of administrative and operation activities to support the PMS to the state or state-designated contractor, Team NewWave will develop a detailed Turnover Plan for state approval. The plan will include status reporting of turnover activities and a Turnover Results Report.
5.18.20	Our team's Key Personnel and corporate experience in executing project management, systems integration, and development processes and methodologies provides the state with a high level of confidence in our ability to deliver the solution per contract requirements.
5.18.20.1	Team NewWave's project manager will plan for and ensure qualified staff are delivering documents, services, and support in the approved PWP. We will meet the due date (as described in the PWP) of acceptance of all deliverables; this is a NewWave corporate requirement as well as a PMS requirement.
5.18.20.2	As is our common practice, Team NewWave will distribute meeting agendas at least 24 hours before the scheduled meeting and will distribute meeting minutes, including action items and decisions made, to the attendees within 2 business days of the meeting.
5.18.20.3	Team NewWave has deep reach-back capability to each of our corporate resources, as well as strong recruiting teams to ensure key Personnel positions are not vacant for more than 10 days. We establish succession and contingency plans for any Key Personnel vacancy. We will obtain the state's approval for any replacement staff and ensure they have qualifications equal to (or exceeding) the qualifications of the person being replaced.
5.18.20.4	Team NewWave tracks all priority tickets and their due dates before completion to ensure on-time delivery.
5.18.20.5	Team NewWave understands that testing is vital in software systems development, and we have a reliable system that ensures we meet all requirements. To implement a system without a significant testing plan can damage a system's entire operational performance. Team NewWave is committed to developing a complete and robust testing plan to ensure our solution performs to the highest standards. As a best practice, we will provide multiple environments to "promote" changes through rigorous test phases. These environments include development, QA, integration, and production. See Section A.12 for our proposed approach to managing these environments. Team NewWave will maintain accurate configuration and extensions records across all environments. Using our environment scanning tools enables us to prepare update packages and deploy them to each environment in a proactive way to ensure every deployment is thoroughly tested and there is minimal to no production downtime.
5.18.20.6	IBM Cúram provides visual tools that will allow identified and trained state users to configure business rules and processes, including a rules editor for eligibility rules, a workflow process definition tool for managing and configuring workflows, and an IEG editor for creating and maintaining provider application scripts and wizards.
5.18.20.7	Team NewWave will develop a Change Management Plan for AHCCCS/Med-QUEST approval within 60 calendar days from the contract execution date. The plan will be maintained throughout the life of the contract and will include the following: • Written, trackable, and diagrammatic representation describing the processes and procedures to be used to initiate, evaluate, review, and resolve any change requests that occur, both before and after the PMS is implemented • Best practices guidelines for change management, as described in ISO/International Electrotechnical Commission (IEC) 20000 [1 to 11] standards for Information Technology Service Management, which is contained within the ITIL framework. The Configuration Items (CI) list in the Configuration Management Plan will identify each CI's specific requirements. All documentation will be stored in SharePoint with controlled access and will be available for viewing and download via the PMS Project Management Portal.

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

A.18.a Project Management Plan

Our Project Management Plan (PMP) provides the management framework to initiate, plan, control, and monitor contract activities so that all deliverables, artifacts, and reviews are consistent with our certified best practices. We will tailor our PMP and PWP to align with AHCCCS/Med-QUEST requirements for driving successful program execution. See Appendix B for our draft PMP for the PMS project.

A.18.b Project Work Plan (Gantt Chart)

The draft PWP Gantt Chart (Figure 5) identifies the major activities for the PMS project. To conserve space, we provide the tasks and timelines for the first year of the contract. This includes 9 months for implementing our solution and 3 months of post-implementation support. The tasks for providing post-implementation support in years 2–5 will mirror the post-implementation tasks of year one. See Appendix C for our draft PWP task list schedule for the PMS project.

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

TASKS
Provider Management System
09.02.2018–09.15.2019

2018: SEP, OCT, NOV | 2019: DEC, JAN, FEB, MAR, APR, MAY, JUN, JUL, AUG, SEP

- 1.3.2.13.3.5 – Fine Detailed Design Review
- 1.3.2.13.3.6 – Data conversion analysis & conversion plan
- **1.3.2.13.4 – Development**
  - 1.3.2.13.4.1 – Portals for state worker access, Provider enrollment/registration & reporting
  - 1.3.2.13.4.2 – User training plan (knowledge transfer, desktop manuals, on-site training)
  - 1.3.2.13.4.3 – Contingency Plan/Recovery Plan
- **1.3.2.13.5 – Testing & Evaluation**
  - 1.3.2.13.5.1 – Test plan for functional, integration, system, regression & user acceptance testing
  - 1.3.2.13.5.2 – Validation of test reporting
  - 1.3.2.13.5.3 – Error reporting & remediation planning for test stages
- **1.3.2.13.6 – Implementation**
  - 1.3.2.13.6.1 – Implementation/Roll out plan to include dashboard reporting
  - 1.3.2.13.6.2 – Validation of production reports
  - 1.3.2.13.6.3 – Ongoing error reporting
  - 1.3.2.13.6.4 – SLA agreements
- **1.3.2.13.7 – Post Implementation**
  - 1.3.2.13.7.1 – Post implementation plan for both AHCCCS/Med-QUEST
  - 1.3.2.13.7.2 – Post implementation documentation for delivery
  - 1.3.2.13.7.3 – Post implementation support/maintenance plan
  - 1.3.2.13.7.4 – Error reporting & remediation planning
- **1.3.2.13.8 – IV&V Coordination & Reporting**
  - 1.3.2.13.8.1 – Timely response to all request from IV&V
  - 1.3.2.13.8.2 – Quarterly reporting
  - 1.3.2.13.8.3 – Milestone reporting
  - 1.3.2.13.8.4 – Develop & deliver a plan for CMS Certification

1.3.3 – System Security

- 1.3.3.1 – Ensure compliance with AHCCCS/Med-QUEST security policies & operations
- 1.3.3.2 – Maintain security architecture
- 1.3.3.3 – Provide Security Awareness Training
- 1.3.3.4 – Perform security monitoring & evaluation
- 1.3.3.5 – System Security Plan (SSP)
- 1.3.3.6 – Contingency Plan (CP)
- 1.3.3.7 – Contingency Plan (CP) Tabletop Test After Action Report (AAR)
- 1.3.3.8 – Plan of Action & Milestones (POA&M) as required
- 1.3.3.9 – Corrective Action Plan (CAP) as required
- 1.3.3.10 – Information Security (IS) Risk Assessment (RA)
- 1.3.3.11 – Background Investigation Status Report as required
- 1.3.3.12 – Risk Vulnerability Assessment (RVA)

1.3.4 – PMS Implementation

- 1.3.4.1 – Sprint 0
- 1.3.4.1.1 – Develop prioritized Epics
- 1.3.4.1.2 – Develop prioritized Features
- 1.3.4.1.3 – Develop prioritized user stories for Sprints

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

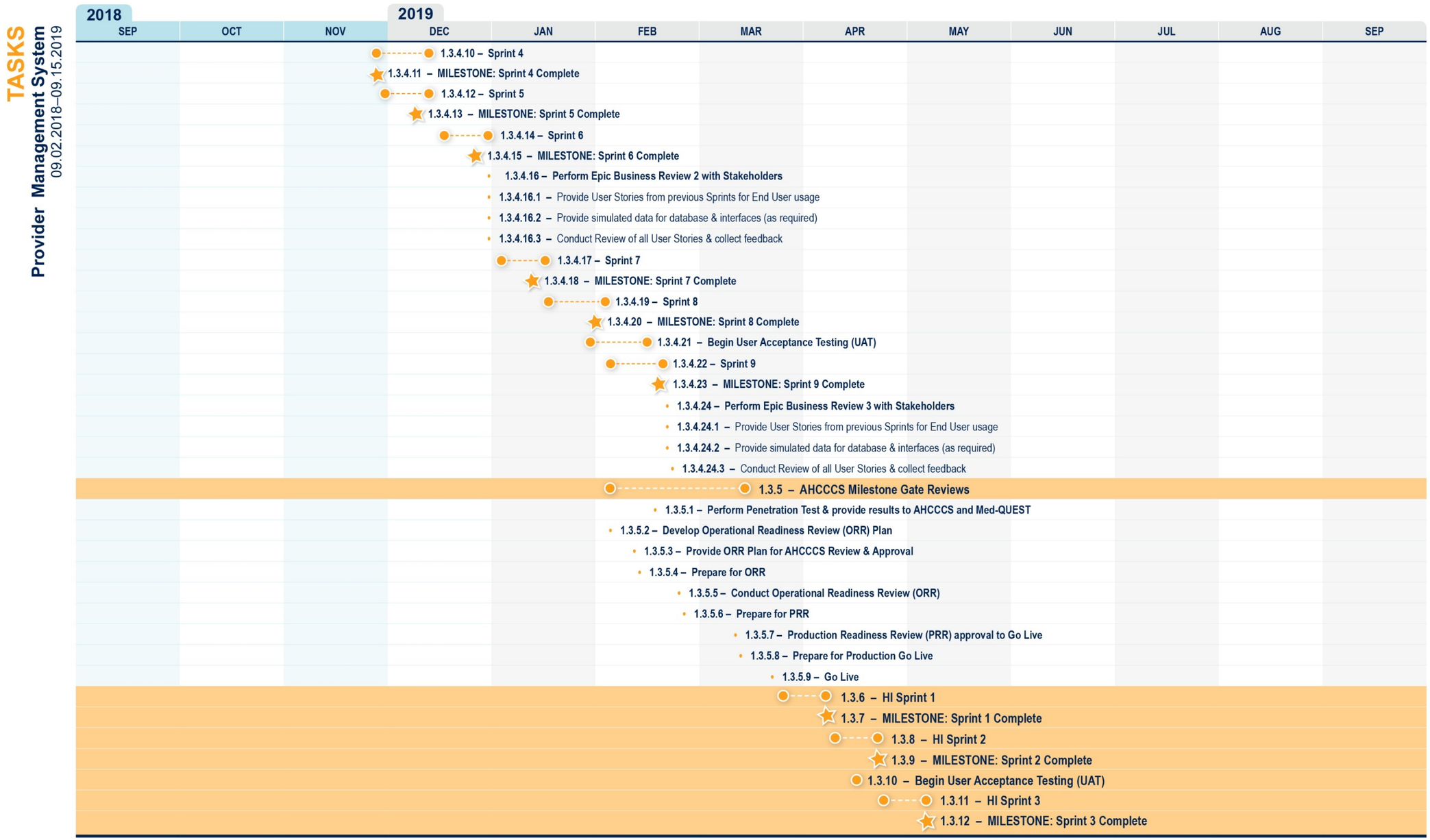
TASKS

Provider Management System
09.02.2018–09.15.2019

2018			2019									
SEP	OCT	NOV	DEC	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP

- **1.3.4.1.4 –** Conduct JAD Sessions
- **1.3.4.1.5 –** Develop & deliver UAT Test Plan
- **1.3.4.1.6 –** Establish & groom Product backlog
- **1.3.4.1.7 –** Implementation Schedule
- **1.3.4.1.7.1 –** Draft Epic, Feature & Sprint Schedules
- **1.3.4.1.7.2 –** Conduct internal review of Schedules
- **1.3.4.1.7.3 –** Incorporate internal feedback into Schedules
- **1.3.4.1.7.4 –** Review & Baseline Schedules with AHCCCS/Med-QUEST
- **1.3.4.1.7.5 –** Submit Epic, Feature & Sprint Schedules to AHCCCS/Med-QUEST
- **1.3.4.2 – MILESTONE: Planning Sprint 0 Complete**
- **1.3.4.3 – Sprint 1**
  - **1.3.4.3.1 –** Sprint Planning
  - **1.3.4.3.2 –** Discovery (Develop user, business & system requirements)
  - **1.3.4.3.3 –** Design (Architect, software components/modules, interfaces and/or database)
  - **1.3.4.3.4 –** Conduct JAD Sessions
  - **1.3.4.3.5 –** Implement Sprint Tasks
  - **1.3.4.3.6 –** System Integration Testing
  - **1.3.4.3.7 –** Sprint Review & Retrospective
- **1.3.4.4 – MILESTONE: Sprint 1 Complete**
- **1.3.4.5 – Sprint 2**
  - **1.3.4.5.1 –** Sprint Planning
  - **1.3.4.5.2 –** Discovery (Develop user, business & system requirements)
  - **1.3.4.5.3 –** Design (Architect, software components/modules, interfaces and/or database)
  - **1.3.4.5.4 –** Conduct JAD Sessions
  - **1.3.4.5.5 –** Implement Sprint Tasks
  - **1.3.4.5.6 –** System Integration Testing
  - **1.3.4.5.7 –** Sprint Review & Retrospective
- **1.3.4.6 – MILESTONE: Sprint 2 Complete**
- **1.3.4.7 – Sprint 3**
  - **1.3.4.7.1 –** Sprint Planning
  - **1.3.4.7.2 –** Discovery (Develop user, business & system requirements)
  - **1.3.4.7.3 –** Design (Architect, software components/modules, interfaces and/or database)
  - **1.3.4.7.4 –** Conduct JAD Sessions
  - **1.3.4.7.5 –** Implement Sprint Tasks
  - **1.3.4.7.6 –** System Integration Testing
  - **1.3.4.7.7 –** Sprint Review & Retrospective
- **1.3.4.8 – MILESTONE: Sprint 3 Complete**
- **1.3.4.9 – Perform Epic Business Review 1 with Stakeholders**
  - **1.3.4.9.1 –** Provide User Stories from previous Sprints for End User usage
  - **1.3.4.9.2 –** Provide simulated data for database & interfaces (as required)
  - **1.3.4.9.3 –** Conduct Review of all User Stories & collect feedback

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.



Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

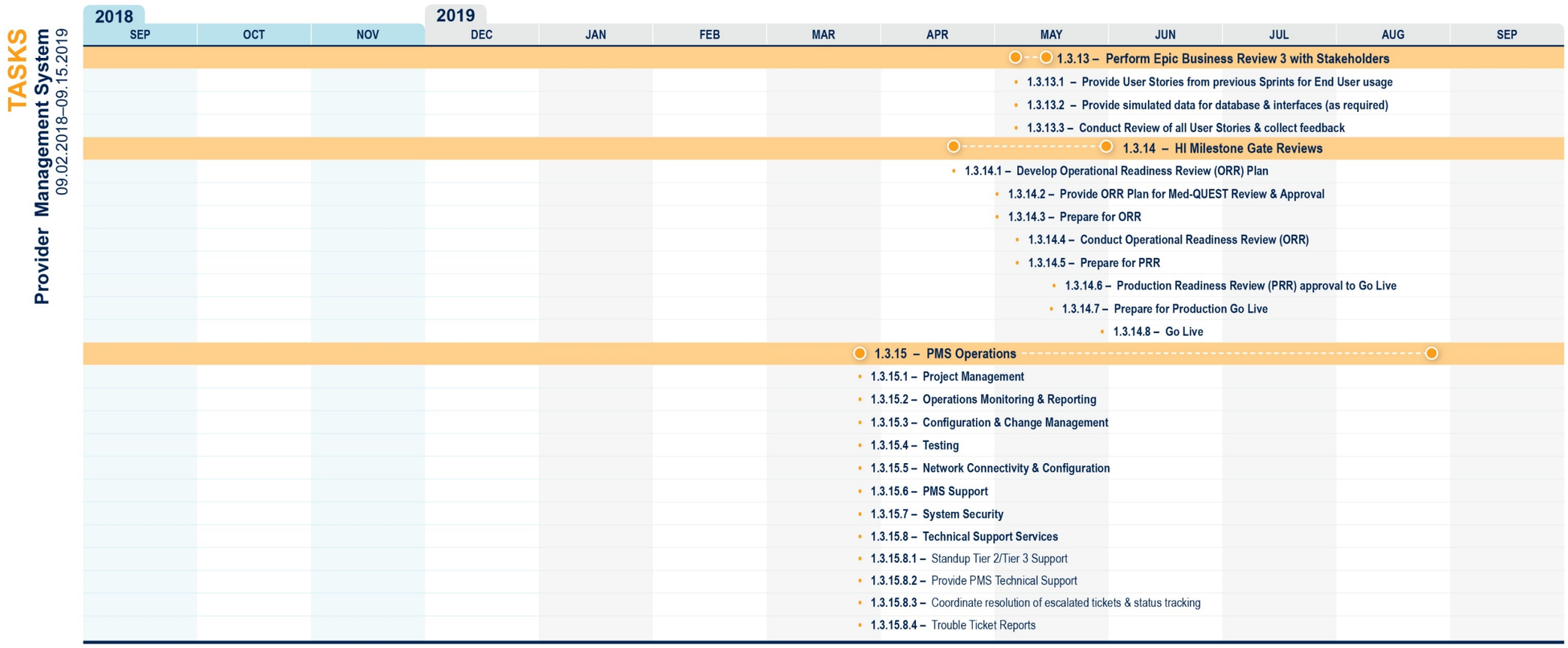


Figure 4: Gantt Chart for Provider Management System Implementation

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

A.19 TRAINING (SOW 5.19)

A key tenet of our approach to large system training is to provide users with training information that resonates with their work as well as the tools necessary to effectively apply the training in work-specific applications. Training often incorrectly focuses on system functionality in isolation, thereby delivering a standard training approach. Our team avoids this pitfall through role-based training, which is the most effective approach because it puts training in the context of each individual job role. Strong users develop over time, and we focus our approach on training and coaching to meet the needs of the end users.

System Fundamentals: We design the first level of training for a broad range of users. The training provides a solid foundation for using all tools in the solution, with instruction focused on the specific users and uses of each tool. We assess the broader user community and work with the client to target users for education and analytic development.

Integration: For the second training level, we take a more customized approach to help users integrate their tool knowledge and other information into their daily workflow. We target power users and program managers who use data to inform their day-to-day business decisions by providing training that focuses on specific functional areas, such as provider enrollment.

Expertise: This level of training is more focused and builds on previous user experience. It allows users to master the tools and maximize the analytic application of the solution to their specific program areas. Users at this level are functioning independently, using tools in our analytic toolkit, and are prepared for involvement in all aspects of the Provider Management System (PMS). These users interact with our training team and SMEs to discuss scenarios specific to their program areas. This level of training encompasses the professional development we believe can change the way managers view information—that is, as a tool to help them become expert users of health information and improve the success of their program management efforts.

Training Plan: Before implementing our solution, we develop and deliver a Training Plan for review and approval. The Training Plan outlines both Design, Development, and Implementation (DDI) and ongoing training approaches, tools, timing, and durations. We train authorized users, ranging from business and technical specialists to managers and directors.

Once we have a final breakdown of your user groups and their business needs, we work with you to develop a detailed training calendar that indicates the training dates, times, courses, and locations. We post the training calendar and related news in your project SharePoint in the training section and include reference guides, pre- and post-classroom exercises, and other appropriate training materials.

The Training Plan identifies agreed-on training parameters and user roles for each of the AHCCCS/Med-QUEST components. We provide both onsite classroom training and web-based training. We provide hard copy training manuals for classroom use and make electronic copies available. Each session includes hands-on activities with coaching from our staff. Users can practice with training data that produces predicable results. As the session ends, users complete an anonymous survey assessing the effectiveness of the training program and instructor, which we compile and deliver to you.

In addition to the detailed training calendar, the Training Plan incorporates mutually agreeable training parameters and user roles. It addresses the following items.

Understanding the Underlying Database: Part of each new user training session is devoted to familiarizing attendees with the database structure, data dictionary, and metadata. We address key data quality findings and their implications for analysis. Because we have found that business analysts often are not knowledgeable about claims and encounter data, we offer a targeted course on this topic.

Specific Tools, Targeted to User Types and Levels: We train users on each tool in our solution, with different courses for different types of users—executives, program managers, business analysts, power users. Courses cover everything from logging on to the system, to applying functionality relevant to the user's job responsibilities. Users practice with training data that produces predictable results. We distribute hard copy training manuals for classroom use, along with electronic copies. Each session features hands-on activities with coaching from our staff; we examine specific case studies identified during business analysis (e.g., monitoring managed-care organizations or detecting provider fraud and abuse). To facilitate instructor interaction, we typically limit the hands-on training to 10 users per session.

Training Delivery Formats: To encourage continuous learning, we provide an Internet-accessible healthcare knowledge base with analytical guides and job aids, such as Tips and Tricks, FAQs, newsletters, and user alerts. Our "shoulder-to-shoulder" coaching and networking help your staff learn from experts and our other clients. We closely monitor system usage by business unit; if usage decreases, we will alert you and intervene to develop correction plans.

Ongoing Training: Continual training is key to successful use of the PMS solution throughout the life of the contract. Our proposed training schedule foresees three annual training sessions, allowing for continued dissemination of updated or new functionality or business processes throughout the term of the contract.

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

Team NewWave's tiered approach to training not only teaches users on the system components, but also helps staff members learn to apply the information in their daily work to increase efficiency and productivity.

SOW	Team NewWave Response
5.19.1	According to the implementation schedule, Team NewWave will provide training for AHCCCS/Med-QUEST and Provider Registration staff as agreed with AHCCCS/Med-QUEST. We will work collaboratively to establish a Training Plan that delivers an appropriate curriculum and the content required by the project. Refer to Section A.19 for a detailed description of our training methodologies.
5.19.2	During implementation and transition to the new PMS, Team NewWave will assist with and participate in education, training, and communication, and as needed going forward to support system changes. We will work collaboratively to establish a Training Plan that delivers an appropriate curriculum and the content required by the project.
5.19.3	Team NewWave engineers will provide technical training and documentation so the agency and other contractors can use dashboards, reports, and other monitoring tools.
5.19.4	Based on schedules, time availability, and logistics, Team NewWave will establish a Training Plan that delivers an appropriate curriculum and the content required by the project.
5.19.5	Based on regular updates and maintenance to the system, Team NewWave will maintain and update the training environment with training data to use during user training.
5.19.6	To ensure consistency in communication and training, Team NewWave will provide train-the-trainer sessions for agency personnel responsible for training.
5.19.7	If there are significant system impacts on user interaction, Team NewWave will provide training to support new functionality and/or major software releases.
5.19.8	To ensure requirements definition, training, and implementation, Team NewWave will provide onsite support.

A.20 TESTING (SOW 5.20)

SOW	Team NewWave Response
5.20.1	Team NewWave uses multiple environments to perform robust and extensive testing (i.e., development testing, integration testing, system testing and regression testing). We conduct various levels of testing within these environments (i.e., unit testing in the development environment, functional and non-functional system testing in the QA environment) before releasing code into production. We use these testing environments throughout the development stage to ensure code is tested in lower environments through higher environments. We identify and document defects to ensure the defect rate decreases as testing continues in the higher environments. The testers develop positive and negative testing scenarios in all environments. After the code has been tested and has passed in lower environments, it is moved through different testing environments until it reaches the regression testing (staging) environment. This is done to ensure the new (or revised) software does not disrupt current functionality, and that it is compatible with existing processes and interfaces. Thus, before changes are executed in production, they undergo a minimum of three cycles of testing, including one round of integration testing.
5.20.2	Team NewWave understands the complexity of system integration. Our development and testing staff have had great success in implementing and testing interfaces across various applications and data sources within CMS. There are various Team NewWave projects whose systems integrate with CMS' shared services infrastructures. The integration of the system and its inbound and outbound interfaces is tested to ensure security and data integrity. Leveraging our DevOps and Continuous Integration and Continuous Delivery (CI/CD) capabilities, a suite of automation tests is triggered to test our solution as part of the deployment pipeline to ensure data accuracy and interoperability.
5.20.3	Team NewWave understands the complexity of integrating systems. There are various projects at NewWave whose systems integrate with the CMS shared services infrastructures. Testing the interdependencies of systems is conducted on an ongoing basis to ensure the introduction of new code has not disrupted the system. The integrated systems will be developed, tested, and maintained to ensure data integrity. Team NewWave will work with all

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

	contractors to ensure all testing is coordinated through all layers of responsibilities and that documentation for each level is provided to the AHCCCS/Med-QUEST. Integration testing will be combined with regression testing to ensure there are no breaks in the existing interoperability and data integrity while solutioning for any interdependencies with other systems. Team NewWave will apply the above solutioning and integration processes and policies to all interdependencies that AHCCCS/Med-QUEST may require. Our experienced development and testing staff, who have had great success in developing, coding, and testing the interdependencies with various applications and data sources, will be a great benefit to the AHCCCS/Med-QUEST solution.
5.20.4	Team NewWave will complete and maintain Test Summary Reports (TSR) for all system testing, including tests conducted, tests passed, defects identified, and tests held for future testing. This report will contain defect prioritization based on functionality requirements, and level-of-effort (LOE) estimates for each defect. After performance testing is complete, we compile and deliver all system testing results in a formal meeting for state and state-approved trading partner review. We also will compile a Requirements Traceability Matrix (RTM) after every release cycle that identifies the user story and requirement that was tested and traces it to the test case with the testing results delivered in a user-friendly format.
5.20.5	Our integration environment will mirror the production environment and will be used to conduct user acceptance testing (UAT), automated testing, performance testing (to test responsiveness, reliability, and resource usage), and Section 508 testing (testing to ensure accessibility for users with disabilities). The integration environment will align at all times with the production environment to ensure AHCCCS/Med-QUEST has an environment that is available to perform UAT at all times or to conduct simulations on functionality for internal users.
5.20.6	As part of our test planning, Team NewWave recognizes the need to maintain a roster of the state's key SMEs in each function of provider management to ensure a consistent workflow process from design through UAT. We will facilitate UAT as outlined in the following sub-paragraphs.
5.20.6.1	We will facilitate UAT to provide test cases and scripts from previous test levels.
5.20.6.2	We will assist state personnel in developing UAT test cases.
5.20.6.3	We will provide and maintain a dedicated UAT environment to support continuous UAT throughout design, configure/build, and testing.
5.20.6.4	We will refresh data, execute processes, and migrate releases or code fixes as needed.
5.20.6.5	We will provide test data as required.
5.20.6.6	We will provide AHCCCS/Med-QUEST with a mechanism to enter defects into the online defect-tracking tool.
5.20.6.7	We will maintain a repository of all test documentation, including test scenarios and results.
5.20.7	All test cases and testing results will be recorded in the Zephyr Test Manager tool. Defects will be tracked via Jira. Designated AHCCCS/Med-QUEST staff will have access to both tools.
5.20.8	Designated AHCCCS/Med-QUEST staff will be given appropriate access to the testing environment to conduct independent testing.
5.20.9	Team NewWave will develop test plans and user test scenarios to test each customer-approved implementation requirement during each release. Our testing team will prepare a testing plan to outline UAT, including testing roles, to explain the number of requirements tested in the release, to trace each scenario to a development requirement, and to provide a state-approved UAT schedule. Team NewWave will develop each scenario in conjunction with state business owners.
5.20.10	Part of the DevOps CI/CD pipeline will be automated execution of integration testing. Team NewWave will coordinate the effort with AHCCCS/Med-QUEST subsystem owners and ensure no new code changes break inter-component dependencies.
5.20.11	Team NewWave's testing team will develop test plans and testing data for various projects. Within the plan, the

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

	various levels and environments for testing are detailed. Our test team will work with the state to prepare set testing statistics to track (e.g., number of tests forecasted, number of tests performed, percentage of defects identified) and set as standard algorithms to be included for each testing effort as expected outcomes. Team NewWave will document an agreed-on schedule to ensure ample time is allotted to test in all environments for each release (development, integration, QA, and VAL). All test results will be reviewed and documented with the customer to ensure each party agrees with the test results and any mitigation plans required. The final test documents (test plan, test scripts, and testing results) will be pulled together by our testing team and delivered to the customer within a required time frame.
5.20.12	UAT is the last phase of software testing. It is vital for the customer and user to test and understand the system functionality before the move or opening of the system to a production environment or real-time performance. Test plans and user test scenarios are developed to test each requirement that the customer has approved for implementation during each release. Our experienced team of testers prepares a testing plan to outline the strategy for UAT, which would include the roles involved in testing, number of requirements being tested and included in the release, number of scenarios that would be developed tracing back to each requirement, and a state-approved schedule for the UAT. NewWave will develop each scenario in conjunction with the state business owner. During the UAT sessions, any defects, modifications, or concerns will be documented by NewWave and a plan for remediation will be developed with sign-off from the state. Once all corrections and adjustments are complete, retesting of the system in the VAL environments will be scheduled to obtain the final sign-off for deployment to production. The final sign-off will be regarded as the state's approval that the system meets all requirements tested and are to be implemented for a release. We will share all documents with our customer based on an agreed-on time frame.

A.21 MAINTENANCE/ OPERATIONS (SOW 5.21)

SOW	Team NewWave Response
5.21.1	Team NewWave's preferred tool for processing change requests, implementation progress, and defect tracking and reporting is Atlassian's Jira. Cherwell Service Management integrates with Jira by linking business objects in Cherwell to issues in Jira. For IBM Cúram–related upgrades, later versions of Cúram, Fix Packs, and iFixes are all released with a detailed list of changes in the release notes, are publicly available on IBM's Support website. With major releases, an updated IBM Cúram Upgrade Helper is also published. The Upgrade Helper is a set of tools, documents, and guides that assist in upgrading both the source code and the application database schema. It has detailed and specific migration paths and tasks to execute based on the current version and the target version. Using the Upgrade Helper pack in conjunction with the Cúram compliance guide, all new data items and project-level product extensions are added to the migration path during a software upgrade.
5.21.2	The Cúram OOTB install ensures consistency across all user screens, reports, and database tables. Team NewWave is committed to working with both Hawaii and Arizona to ensure that project-level extensions maintain consistency throughout. One tool we use to help maintain consistency is the Cúram Analysis Documentation Generator (CADG) tool, which is available to download the solution IBM's Fix Central. It allows users to explore the metadata associated with pages and database tables, along with information about related artifact types, such as Tabs, Domain Definitions, Code Tables, Message Files, Application Properties, and Workflows. Business users and administrators can use this tool to assess the impact and ensure consistency of terminology and messaging when designing functionality associated with the AHCCCS PMS.
5.21.3	Cúram natively supports effective date for all configuration changes. These are stored in the DB2 database and can be either future dated or retroactive. Users have the ability to specify data edits by type of transaction. All changes in the solution are maintained in an effective-dated manner, ensuring that changes are tracked over time. Many other functions within Cúram also follow this approach where appropriate.
5.21.4	Team NewWave will provide a dashboard for system job, maintenance schedule, submission, and processing statics to designated state staff along with access to system performance tools.

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

5.21.5	Section A.24 discusses in depth Software Configuration Management (SCM). Using proper SCM techniques, Team NewWave ensures all project source artifacts are tracked in a Git repository. During project implementation, developers may be checking code in and out, giving rise to a possibility that one or more combined changes may result in a bug. When appropriate, these code commits can be reversed using the SCM capabilities of Git, thus reversing the changes that gave rise to the bug. If a bug is discovered after a software update, such as an iFix, Team NewWave will similarly use the appropriate SCM techniques, such as tagging repositories, to reverse the software update. Team NewWave will have a restoration plan for any change made to the system. We will take a backup of both the data and the system state before any change that affects any system and provide a detailed restore procedure in the event the data or systems become unusable or unstable and the data or system needs to be reverted to the pre-change condition.
5.21.6	The system is capable of outcome-based and rule-based processing. It can be configured so that each job is processed based on the outcome of previous jobs.
5.21.7	Team NewWave's Document Management Plan is described in the PMP. The Documentation Management Plan describes overarching requirements, such as media storage, scanning requirements, state agency records management requirements, review and approval process, retention, and access requirements and limitations. The Configuration Items List in the Configuration Management Plan will identify each document's specific requirements and, based on each requirement automated backup, retention, and safe discarding of data, images, and documents will be implemented. This solution is capable of varying retention periods based on the type of data and will be configured to meet the requirements of the AHCCCS/Med-QUEST.
5.21.8	All inter-component communications between each system layer will be encrypted (Secure Socket Layer [SSL]), including file transfer using File Transfer Protocol (FTP).
5.21.9	By using the IBM Integration Bus (IIB), data from multiple sources can be received via various protocols and data formats. IIB supports SOAP, HTTP, and JMS protocols and a wide variety of data formats, including standards-based formats (e.g., XML, DFDL, and JSON), industry formats (e.g., X12, HL7, EDI, SWIFT), and custom formats. Data files can be exchanged via HTTP, HTTPS, FTP, and SSH File Transfer Protocol (SFTP).
5.21.10	Team NewWave's solution supports a wide variety of built-in methods for verifying system integrity and data quality, and for tracking data and transactions that modify system data. The new solution provides database table auditing, business function auditing, and workflow activity auditing that tracks, and traces actions performed by users and processes. The system's auditing and tracking capabilities are configurable to meet the state's future business needs. Team NewWave will build customer interfaces to allow viewing and extraction of audit trail information to meet state-specific requirements.
5.21.11	Using IIB, data can be imported or exported in various formats, including CSV, JSON, XML, EDI, and others.
5.21.12	Our solution has a calendaring and scheduling feature within the application to facilitate meetings and activities related to their work with providers. Team NewWave will integrate the solution's calendaring capabilities with both Arizona and Hawaii's Outlook calendaring system by exporting application calendar entries into vCalendar format, which can be imported into Outlook. Using a similar technique, Outlook entries will be imported into the application calendar as well.
5.21.13	The system will support importing and exporting of data in CSV, XML, and JSON formats. For example, using the solution batch architecture, a batch job can be configured to export a flat file as a Comma Separated Value (CSV) formatted file, which can easily be opened in Microsoft Excel. Similarly, the batch job can import files. Another example is using the solution's built-in communication generation capability to produce PDF files that can be opened using Adobe Acrobat. Using this same technique, other common file formats can be accommodated.
5.21.14	Team NewWave will deploy New Relic, an advanced monitoring tool, that provides application performance and system load insight. Using Azure cloud platform, Team NewWave will ensure auto-scaling scripts provide enough resources to meet system demands, while scaling down resources (when there is minimal load) to save costs. Real-time monitoring will send notifications to log and report irregularities, and automated script will respond to resolve any issues to meet SLAs per AHCCCS/Med-QUEST requirements. Our proposed architecture includes high-availability as

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

	well as a separate region for components and data needed to support continuity of service.
5.21.15	We will leverage Jira to track defects, bugs, and issues found in the testing and production environments. We will ensure designated state staff have full visibility into system support activities and will assign severity levels to tickets for agreed-on SLAs, or as prioritized by the Change Control Board.
5.21.16	For network monitoring, we will deploy PRTG, a powerful tool used for local area network (LAN), wide area network (WAN), wireless LAN (WLAN), and virtual private network (VPN) monitoring. Using PRTG, we monitor network availability and bandwidth usage, in addition to various network parameters such as quality of service, memory load, and CPU usage. PRTG provides system administrators with real-time metrics of various network devices: both physical and virtual. Following is a list of some of the services provided by PRTG: • Monitoring and alerting for uptime or downtime or slow servers • System health monitoring of virtual servers • Network device monitoring and bandwidth accounting • SLA monitoring New Relic and Splunk provide real-time system performance metrics. New Relic provides system response time, throughput, and error rates without going through a list of monitoring tools and application log entries. It is possible to view the application performance trend in one place, including page load times, error rates, slow transactions, and the list of servers running the application. New Relic also identifies and provides reports on slow SQL queries. Using the report, performance bottlenecks can be identified and remedied, allowing for more efficient resource utilization and improved response time. Deployed along with New Relic, Splunk is an engine for machine-generated IT data that provides real-time visibility into the large-scale distributed infrastructure. It collects logs and key metrics from each application layer, including the following: • Cloud configurations, logs, and metrics • Application configurations, logs, and metrics • OS logs and metrics • Network device logs, SNMP traps, and metrics • Storage access and host-level logs Splunk provides monitoring, correlation, and troubleshooting across every layer of the stack with key performance indicators. It provides deep drill-downs, statistical analytics, and real-time dashboards for anyone within the organization. The data collected by Splunk can be used to proactively monitor problems before they affect the system.

A.22 Business Process Redesign

Team NewWave leverages all the benefits of implementing a COTS solution for AHCCCS/Med-QUEST. Based on our extensive implementation experience, as described in our Past Performance, we have a proven approach to working with users toward integrating the Team NewWave solution into the organizations. Our approach is nimble and fully complements our iterative implementation methodology and schedule, while also being able to adapt to meet implementation-specific needs.

Requirements Elaboration and Fit-Gap Analysis - Team NewWave will work in partnership with AHCCCS/Med-QUEST stakeholders and SMEs to review their business requirements against all components of our proposed solution. Using AHCCCS'/Med-QUEST's business requirements as a starting point, we will identify the key functional areas that our work products will be broken down into and review the level of fit for each requirement. The goal is to gain a collective understanding of the requirement and determine if it needs to be broken down further in detail or obsoleted from the scope of the project. During this process, we classify each item in one of three ways: (1) met as part of the base product (i.e., OOTB), (2) met via product configurations, or (3) met via extensions to the product. We will submit our output to the state and obtain agreement with and sign-off by the state and Team NewWave. As a direct result of this step, the process outputs will include the following:

- Signed-off set of business requirements
- Signed-off fit-gap analysis spreadsheet
- Fit-gap analysis summary identifying key areas of fit, and potential gaps.

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

As-Is Process, To-Be Process, and Design - Using the functional areas defined and documented during requirements elaboration and fit-gap analysis, we will work with AHCCCS/Med-QUEST to review the as-is business process flows across these functional areas using any existing pre-defined documentation, with a goal of working toward consistent flows across all functional areas.

Team NewWave will initiate Joint Application Design (JAD) sessions at this stage with stakeholders and SMEs across all functional areas. It is important that the state project team selects a group of individuals to participate in the JAD sessions and Business Process Redesign (BPR) based on their experience, program knowledge, and ability to offer constructive feedback. This participation is important because many of these stakeholders and SMEs will eventually be the super-users on the project (including both onsite and as part of the help desk) during the pilot phase and subsequent location rollouts. This blended state and Team NewWave team will review the as-is process flows in the JAD discussion to develop the to-be business process flows. Using the agreed-on to-be process flows, we will determine whether or not we can minimize a gap through business process change or if we need to design a customized solution to address the gap such that it enables us to develop a consistent set of to-be business processes.

To help the state's team visualize the impact of these decisions, we will demonstrate the OOTB functionalities and design mockup screens, as required, to showcase how we propose to fill some of the identified gaps. The flows, along with our fit-gap analysis, will form part of our robust functional design, Team NewWave's expert technical team will use to implement the PMS.

A.23 Requirements Confirmation

A thorough understanding of requirements is key to the success of the project. Before clearly documenting requirements, Arizona and Hawaii must have a solid understanding of the provider management functionality offered by Cúram OOTB, as well as some common functionality such as workflow, tasks, calendaring, cases, and application. Challenges can arise from an insufficient understanding of the solution components that lead to unnecessary complexity in requirements validation, design, and development. Other challenges can be encountered when business processes do not reflect the system's OOTB business processes. This ties back to the business process redesign, where, in some cases, a thorough understanding of the OOTB functionality may lead to a change in the business process or vice versa; that is, a change to the OOTB process is required.

Team NewWave's approach to requirements confirmation includes the following:

1. Educate participants on what comes OOTB with Cúram in a JAD session in the context of various existing business processes. This helps in requirements confirmation as well as in business process design. Also, once the OOTB business process is understood, it may necessitate a change to the OOTB functionality or a change to the requirements to match what comes OOTB.
2. Have decision-makers and SMEs play active roles in the requirements sessions to keep these sessions on track and productive.
3. Revisit existing requirements; taking into consideration what Cúram offers OOTB. The goal is to always minimize development effort in favor of OOTB functionality. Where this is not possible, key SMEs and decision-makers will be in the room to make the appropriate decisions and to sign-off on the requirements. Once the requirements are signed-off, they serve as a baseline to be used for downstream processes such as design, development, and testing. Team NewWave's agile methodology accommodates situations where a requirement must be revised. In such cases, it may necessitate an update to the downstream processes.

A.24 Software Configuration

IBM Cúram offers in-depth functionality in many areas such as workflow, rules, case management, intake, and more. It is expected from a COTS perspective that some OOTB business processes may need to be altered to suit the business process as required by various project implementations. IBM Cúram has been built with this flexibility in mind, and thus allows extensions in many areas. There are generally two approaches to extending or altering an OOTB business process: through configuration or through extension.

Configuration is the process of altering system behavior through a dynamic online process that may not result in a development build and deployment. An example of a configuration task is to update a description of a code table, which may appear as a drop-down list of values on a screen. The description on a code table can be updated using the built-in online administration

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

suite. A user role defined as the application administrator can log into the system and have access to a range of configuration options. Examples of configurable options are as follows:

- Code tables
- System properties such as logging and tracing
- User profile settings such as name, security role, sensitivity, and many more
- Provider enrollment application scripts (known generically as IEG scripts)
- Business rules such as those rules that may affect issues and verifications against a newly submitted provider application
- Provider communication notice templates, which can be a combination of static and dynamic data.

Cúram also supports a robust Application Development Environment (ADE) that allows extension to the OOTB business processes, or design of a completely new process, using Rational Software Architect (RSA) modeling tool and Java programming language. This technique is used where the Cúram configuration is not applicable; typically, a design review of the functionality will reveal whether or not the task can be handled as a Cúram configuration extension. Cúram development is discussed in-depth as part of the Software Development topic in Section A.25. There is also extensive guidance published online through the IBM knowledge center located at the following URL: https://ibm.biz/BdZH3E.

The benefits of allowing many aspects of system behavior to be altered through configuration follow:

1. Business users can affect a change in the system without involving developer resources. For example:
   - Simple changes such as code table descriptions can be made relatively quickly.
   - More complex changes such as IEG scripts can be changed by business users.
2. Dynamic runtime configuration can greatly reduce the development cycle. In a typical developer cycle, a change needs to be coded, checked into the Software Configuration Management (SCM) repository, built into deployable artifacts, and then scheduled to be deployed. With dynamic configurations, the entire application does not need to be re-built and deployed.
3. Configuration changes can typically be performed and tested more rapidly than development tasks. Applying configuration wherever appropriate helps immensely to meet the proposed timeline for getting the proposed solution for PMS into production.

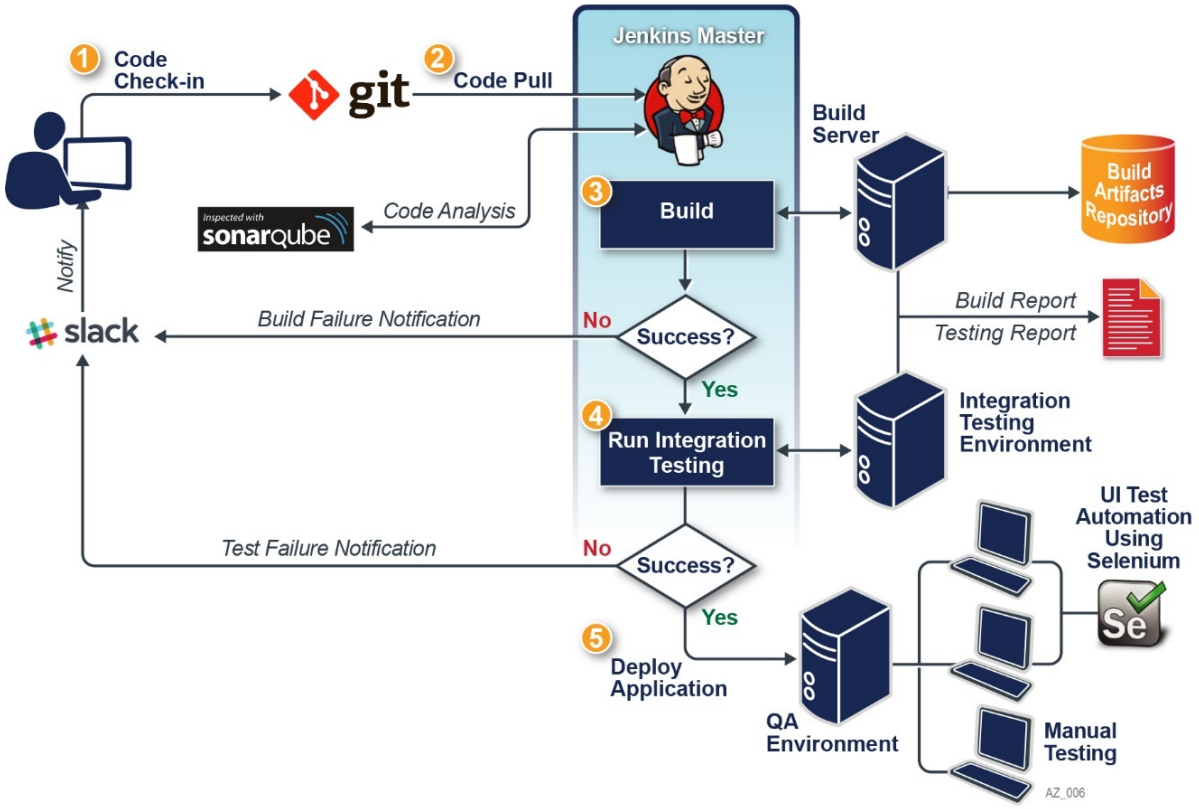
From a SCM perspective, only the source artifacts are managed through the SCM software. For example, the source artifact that contains the UML definition of a Java object is managed through the SCM. The code that is generated by Cúram's build-time scripts is not managed. This is because the generated code is dependent on the source UML and may change dynamically during the build-time. All source artifacts from Cúram and other system configuration files will feed into Team NewWave's DevOps discipline. DevOps is a practice that emphasizes collaboration between developers and the IT team. Both teams work together to automate software delivery and infrastructure changes. One of the outcomes of the DevOps implementation is a CI/CD pipeline, which consists of the following four stages:

1. Code Commit: The developer checks code into the feature branch, which triggers automatic builds to start in Jenkins.
2. Build: The build script (Ant) of the project is executed. If there is an error during the build, a notification is sent to the development team via Slack channel. If the compilation succeeds, unit tests are executed. If any of the unit test fails, then a notification is sent to the development team.
3. Test Execution: All system integration tests are executed in the integration testing environment to ensure successful inter-system integration. If any integration test fails, the development team is notified of the failure.
4. Deploy: When both unit testing and integration testing pass, new code is deployed onto the QA environment for automated Selenium UI testing, functional testing, and regression testing (automated and manual).

A visual overview of the CI/CD process is shown in Figure 6.

Figure 5: Continuous Integration and Continuous Delivery (CI/CD) Pipeline Process Overview

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.



A.25 SOFTWARE DEVELOPMENT (IF APPLICABLE)

Software development is performed in accordance with Team NewWave's agile methodology, as described in our response to SOW 5.18.14. The software development cycle includes the initial set of Cúram configurations plus any required Cúram extension and customization efforts. The Cúram Application Development Environment (ADE) is used to create implementation-specific extensions to the Cúram application. IBM Cúram is highly configurable, but when an implementation calls for extending the original source code, Cúram ADE manages and optimizes the process of extending the OOTB functionality while maintaining the Cúram platform's unique advantages. The starting point for all software development within Cúram is a platform-independent application model, developed using the industry-standard Unified Modeling Language (UML) model. Using a model-driven approach, the tools provided with Cúram minimize the amount of code that must be written and maximize the amount of code that can be automatically generated.

The Cúram development toolset consists of a combination of IBM and open-source products. IBM Rational Software Architect (RSA) is used to perform UML modeling of software components, such as Java classes and Web Service objects. Developers use Eclipse to provide implementation code for the Java classes that are modeled using RSA.

Following the model-driven architecture means all processing in Cúram is accomplished using business process objects (BPO) that are coded in Java. Cúram delivers thousands of BPOs designed specifically to support Arizona and Hawaii's proposed solution and business processes in its reference model. These BPOs can be used as part of a workflow process, such as those used as part of the provider application submission or can be used as a web service to handle real-time interface logic. When used in a web service, it can serve as a starting point for a services-oriented architecture (SOA). A SOA-compliant solution enables loose coupling between systems, which is one of the factors for adherence to MITA's SOA guidelines.

A.26 SECURITY CONFIGURATION

When developing our PMS solution architecture, Figure 7, Team NewWave understood the importance of addressing the security layers to mitigate security risks. Our PMS application component's architecture includes security design considerations across all layers, including from the Cloud Service Provider, network, and application. We also addressed other security considerations, such as backup and disaster recovery.

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

Our proposed PMS architecture includes high availability as well as a separate region for the components and data needed to support the disaster recovery plan's 4-hour Recovery Point Objective (RPO) and 1-hour to 2-hour Recovery Time Objective (RTO).

Team NewWave has more than 10 years of experience in meeting CMS and HIPAA security and compliance requirements. Our recent experience led to the authority to operate (ATO) we secured and currently maintain for CMS' EPPE, CCW-VRDC, and RADV-CDAT systems. These ATOs required in-depth coverage on the following application requirements:

Infrastructure as a Service (IaaS): The IaaS provider, Microsoft Azure for Government (MAG), received a FedRAMP Joint Authorization Board (JAB) Provisional ATO at the high-impact baseline level, including HIPAA control requirements and a signed Business Associate Agreement (BAA).

Microsoft engaged Team NewWave as a subcontractor to assist Leidos and CMS in testing the CMS MAG secure enclave against CMS requirements at the high-impact level.

Team NewWave is the first CMS contractor to migrate an application to the CMS MAG. The migration will be included as part of the overall infrastructure security controls assessment (SCA) testing to obtain ATO for the MAG, as well as for Team NewWave's RADV-CDAT application.

Microsoft will share the FedRAMP packet and/or security controls documentation with authorized parties. Team NewWave will support the state by sharing information and working with third-party auditors to verify data protection and security measures implemented in the PMS environment.

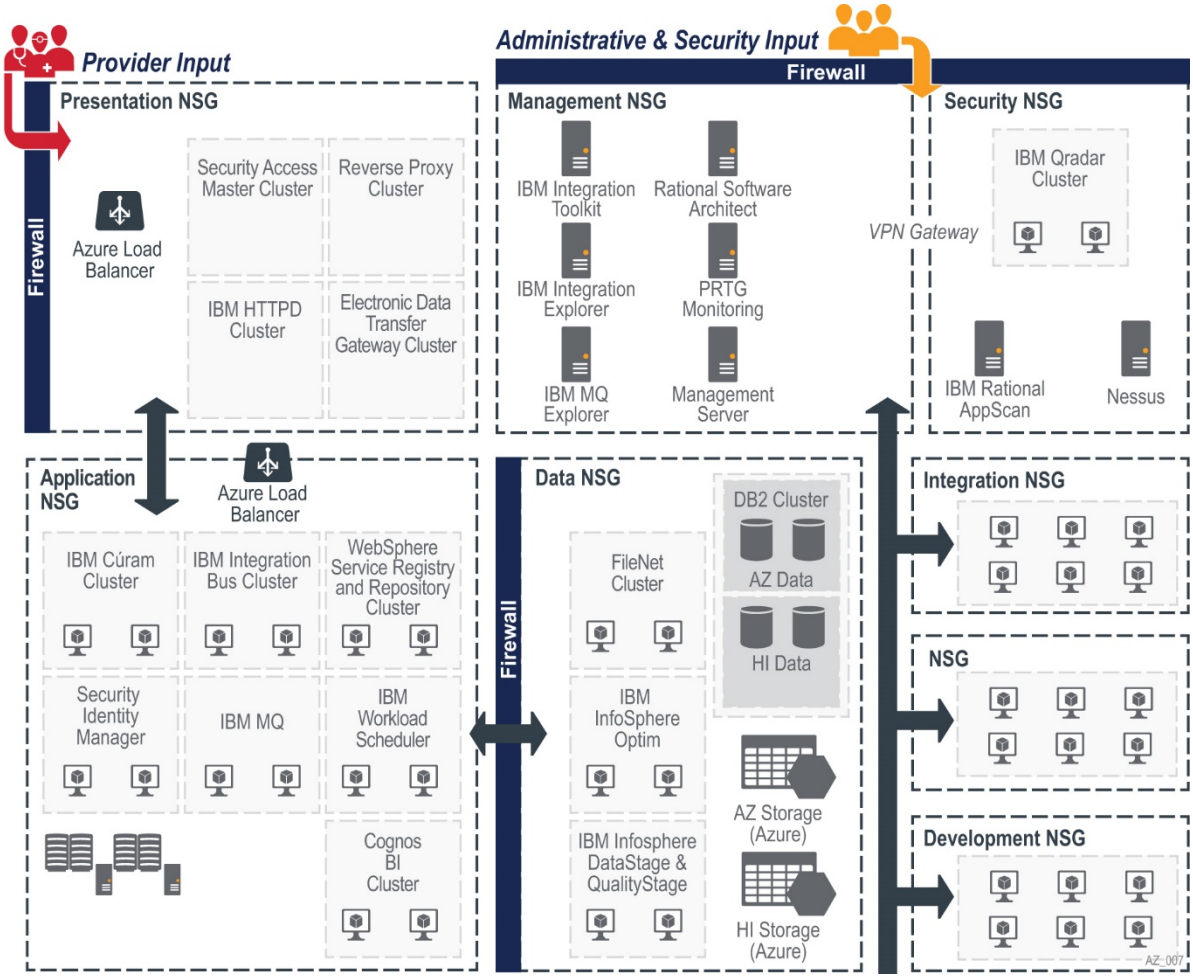


Figure 6: Network Security Architecture

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

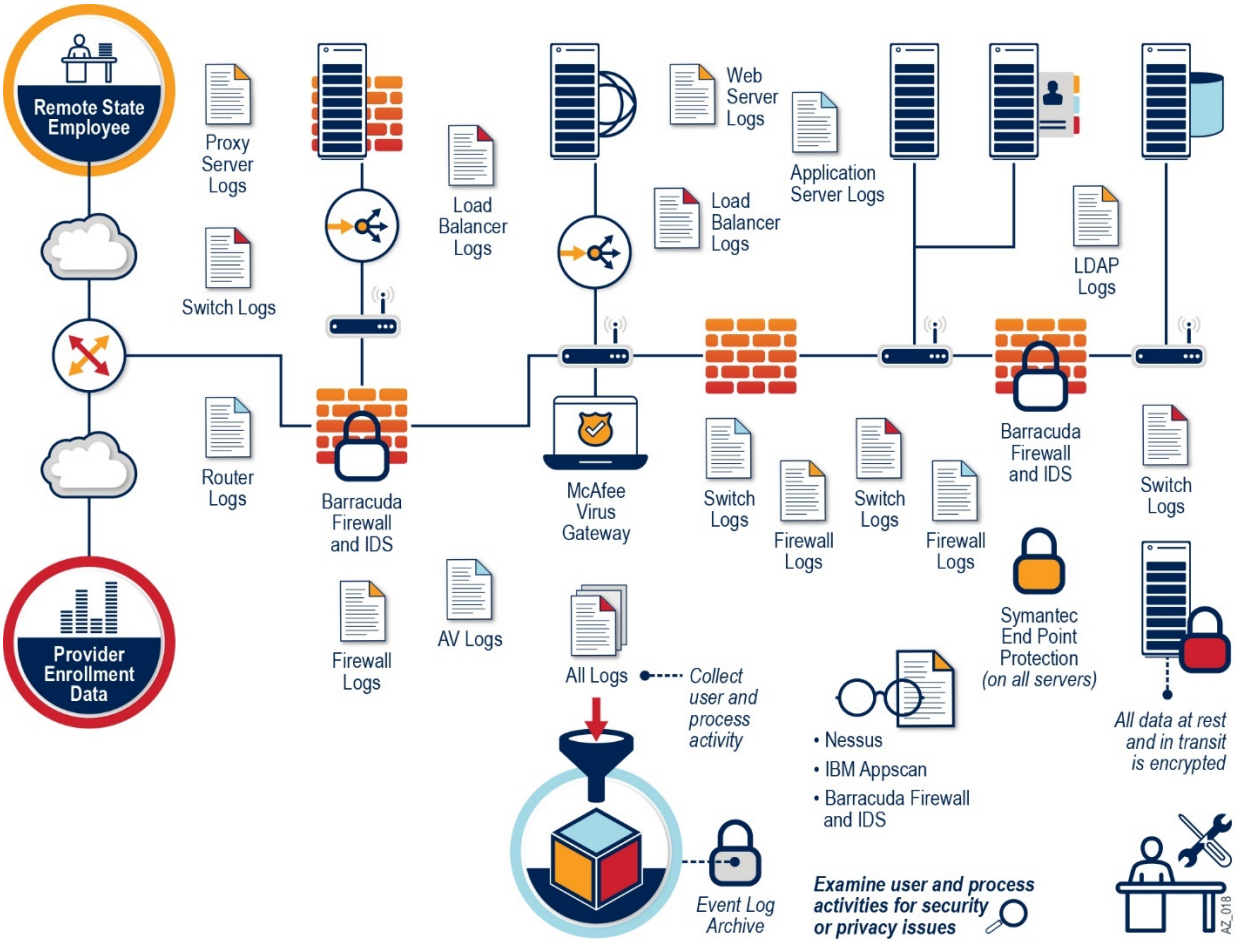
Figure 8 below depicts the tools used to meet the PMS security and privacy requirements. The diagram depicts the system's audit, scan, and trace requirements. Layers of defense are built into the architecture, including the encryption of data at rest and in transit, firewalls between each zone, audit logs of actions detected by every system component, scanning to validate source code, web application, system, and device vulnerabilities, and a security information and event management system (SIEM) that ingests event data from all sources and supports automated notification and user-driven analysis.

Publicly facing entry points. Our proposed application provides firewall-protected access to the presentation zone for business- and mission-related traffic, and firewall-protected access to the management zone for environment administration, monitoring, and security.

Presentation zone is protected by a Barracuda firewall that provides intrusion detection; encrypted traffic is terminated at an Azure load balancer. This zone also contains the McAfee Virus Gateway service, clust

Figure 7: PMS System Security Tools

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.



ered reverse proxy servers, and clustered IBM HTTPD servers. The McAfee Virus Gateway service provides malware detection and network-level protection. Attachments are scanned as they traverse the network and are blocked when they are identified as malware. The reverse proxy to the IBM web (HTTPD) server intercepts web traffic before it reaches the web server, serving as an additional security layer that improves SSL performance, protects Team NewWave's solution from potentially malicious traffic, and abstracts the topology behind the reverse proxy (supporting the ability to change the topology later).

Application zone. Team NewWave's proposed application zone is protected by an Azure network security group (NSG); its traffic is handled by an Azure load balancer. The NSG is Azure's firewall to restrict traffic between zones to the permitted ports and protocols in the NSG rule set. The zone contains clustered implementations of IBM Cúram, IIB, IBM MQ, WebSphere Service Registry and Repository, IBM Workload Scheduler, and Cognos BI. The application zone also includes an Alfresco cluster.

Database zone is protected by a Barracuda firewall and the zone hosts a DB2 cluster containing encrypted system data.

Management zone is protected by a Barracuda firewall and hosts IBM Integration Toolkit, RSA, IBM Integration Explorer, PRTG Monitoring, IBM MQ Explorer, and a management server. Any maintenance on any server components defined in the architecture is performed by an administrator who is logged into the management zone. The NSGs and firewalls prevent remote login to the servers, except from the management zone.

Security zone is protected by a Barracuda firewall. The zone hosts IBM Rational AppScan and a Nessus server. Each of the above zones is protected by a firewall, either a Barracuda firewall (with IDS) or an Azure NSG.

All hosts, applications, NSGs, firewall, and IDS logs are sent to Splunk for log retention, aggregation, consolidation, and correlation. Performance-related event analysis and monitoring are handled by PRTG and New Relic. Splunk integrates with and indexes application performance monitoring (APM) data from New Relic to provide a complete view of the platform environment.

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

IBM Cúram Security: The Cúram application has controls to log user activity at the table and transaction levels. Cúram also leverages other components for rule- and role-based access control (RBAC). A user who wishes to log into Cúram establishes a TLS 1.2 encrypted connection through the reverse proxy to the IBM HTTPD server front end of IBM Cúram. The encrypted connection protects the data exchange and the credentials used to establish a Cúram session.

Cúram will accept the session token that is generated at user login. Once authentication is confirmed, access to backend services, including the Oracle database, are granted and the system retrieves the user's assigned roles and application profiles. The role and application profile defined in Cúram determine what a user can see in terms of interface components, their data access, and their operations. Cúram use a lightweight directory access protocol (LDAP) directory as the repository for user IDs and passwords. This provides a central user repository to grant or revoke access and application permissions. Authentication workflows can support risk-based access control, where a workflow failure can trigger a higher-level workflow, where an additional factor is requested.

Security zone is protected by a Barracuda firewall. The zone hosts IBM Rational AppScan and a Nessus server. Each of the above zones is protected by a firewall, either a Barracuda firewall (with IDS) or an Azure NSG.

All hosts, applications, NSGs, firewall, and IDS logs are sent to Splunk for log retention, aggregation, consolidation, and correlation. Performance-related event analysis and monitoring are handled by PRTG and New Relic. Splunk integrates with and indexes application performance monitoring (APM) data from New Relic to provide a complete view of the platform environment.

IBM Cúram Security: The Cúram application has controls to log user activity at the table and transaction levels. Cúram also leverages other components for rule- and role-based access control (RBAC). A user who wishes to log into Cúram establishes a TLS 1.2 encrypted connection through the reverse proxy to the IBM HTTPD server front end of IBM Cúram. The encrypted connection protects the data exchange and the credentials used to establish a Cúram session.

Cúram will accept the session token that is generated at user login. Once authentication is confirmed, access to backend services, including the Oracle database, are granted and the system retrieves the user's assigned roles and application profiles. The role and application profile defined in Cúram determine what a user can see in terms of interface components, their data access, and their operations. Cúram use a lightweight directory access protocol (LDAP) directory as the repository for user IDs and passwords. This provides a central user repository to grant or revoke access and application permissions. Authentication workflows can support risk-based access control, where a workflow failure can trigger a higher-level workflow, where an additional factor is requested.

Security zone is protected by a Barracuda firewall. The zone hosts IBM Rational AppScan and a Nessus server. Each of the above zones is protected by a firewall, either a Barracuda firewall (with IDS) or an Azure NSG.

All hosts, applications, NSGs, firewall, and IDS logs are sent to Splunk for log retention, aggregation, consolidation, and correlation. Performance-related event analysis and monitoring are handled by PRTG and New Relic. Splunk integrates with and indexes application performance monitoring (APM) data from New Relic to provide a complete view of the platform environment.

IBM Cúram Security: The Cúram application has controls to log user activity at the table and transaction levels. Cúram also leverages other components for rule- and role-based access control (RBAC). A user who wishes to log into Cúram establishes a TLS 1.2 encrypted connection through the reverse proxy to the IBM HTTPD server front end of IBM Cúram. The encrypted connection protects the data exchange and the credentials used to establish a Cúram session.

Cúram will accept the session token that is generated at user login. Once authentication is confirmed, access to backend services, including the Oracle database, are granted and the system retrieves the user's assigned roles and application profiles. The role and application profile defined in Cúram determine what a user can see in terms of interface components, their data access, and their operations. Cúram use a lightweight directory access protocol (LDAP) directory as the repository for user IDs and passwords. This provides a central user repository to grant or revoke access and application permissions. Authentication workflows can support risk-based access control, where a workflow failure can trigger a higher-level workflow, where an additional factor is requested.

Security zone is protected by a Barracuda firewall. The zone hosts IBM Rational AppScan and a Nessus server. Each of the above zones is protected by a firewall, either a Barracuda firewall (with IDS) or an Azure NSG.

All hosts, applications, NSGs, firewall, and IDS logs are sent to Splunk for log retention, aggregation, consolidation, and correlation. Performance-related event analysis and monitoring are handled by PRTG and New Relic. Splunk integrates with and indexes application performance monitoring (APM) data from New Relic to provide a complete view of the platform environment.

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

IBM Cúram Security: The Cúram application has controls to log user activity at the table and transaction levels. Cúram also leverages other components for rule- and role-based access control (RBAC). A user who wishes to log into Cúram establishes a TLS 1.2 encrypted connection through the reverse proxy to the IBM HTTPD server front end of IBM Cúram. The encrypted connection protects the data exchange and the credentials used to establish a Cúram session.

Cúram will accept the session token that is generated at user login. Once authentication is confirmed, access to backend services, including the Oracle database, are granted and the system retrieves the user's assigned roles and application profiles. The role and application profile defined in Cúram determine what a user can see in terms of interface components, their data access, and their operations. Cúram use a lightweight directory access protocol (LDAP) directory as the repository for user IDs and passwords. This provides a central user repository to grant or revoke access and application permissions. Authentication workflows can support risk-based access control, where a workflow failure can trigger a higher-level workflow, where an additional factor is requested.

Security zone is protected by a Barracuda firewall. The zone hosts IBM Rational AppScan and a Nessus server. Each of the above zones is protected by a firewall, either a Barracuda firewall (with IDS) or an Azure NSG.

All hosts, applications, NSGs, firewall, and IDS logs are sent to Splunk for log retention, aggregation, consolidation, and correlation. Performance-related event analysis and monitoring are handled by PRTG and New Relic. Splunk integrates with and indexes application performance monitoring (APM) data from New Relic to provide a complete view of the platform environment.

IBM Cúram Security: The Cúram application has controls to log user activity at the table and transaction levels. Cúram also leverages other components for rule- and role-based access control (RBAC). A user who wishes to log into Cúram establishes a TLS 1.2 encrypted connection through the reverse proxy to the IBM HTTPD server front end of IBM Cúram. The encrypted connection protects the data exchange and the credentials used to establish a Cúram session.

Cúram will accept the session token that is generated at user login. Once authentication is confirmed, access to backend services, including the Oracle database, are granted and the system retrieves the user's assigned roles and application profiles. The role and application profile defined in Cúram determine what a user can see in terms of interface components, their data access, and their operations. Cúram use a lightweight directory access protocol (LDAP) directory as the repository for user IDs and passwords. This provides a central user repository to grant or revoke access and application permissions. Authentication workflows can support risk-based access control, where a workflow failure can trigger a higher-level workflow, where an additional factor is requested.

Security zone is protected by a Barracuda firewall. The zone hosts IBM Rational AppScan and a Nessus server. Each of the above zones is protected by a firewall, either a Barracuda firewall (with IDS) or an Azure NSG.

All hosts, applications, NSGs, firewall, and IDS logs are sent to Splunk for log retention, aggregation, consolidation, and correlation. Performance-related event analysis and monitoring are handled by PRTG and New Relic. Splunk integrates with and indexes application performance monitoring (APM) data from New Relic to provide a complete view of the platform environment.

IBM Cúram Security: The Cúram application has controls to log user activity at the table and transaction levels. Cúram also leverages other components for rule- and role-based access control (RBAC). A user who wishes to log into Cúram establishes a TLS 1.2 encrypted connection through the reverse proxy to the IBM HTTPD server front end of IBM Cúram. The encrypted connection protects the data exchange and the credentials used to establish a Cúram session.

Cúram will accept the session token that is generated at user login. Once authentication is confirmed, access to backend services, including the Oracle database, are granted and the system retrieves the user's assigned roles and application profiles. The role and application profile defined in Cúram determine what a user can see in terms of interface components, their data access, and their operations. Cúram use a lightweight directory access protocol (LDAP) directory as the repository for user IDs and passwords. This provides a central user repository to grant or revoke access and application permissions. Authentication workflows can support risk-based access control, where a workflow failure can trigger a higher-level workflow, where an additional factor is requested.

Security zone is protected by a Barracuda firewall. The zone hosts IBM Rational AppScan and a Nessus server. Each of the above zones is protected by a firewall, either a Barracuda firewall (with IDS) or an Azure NSG.

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

All hosts, applications, NSGs, firewall, and IDS logs are sent to Splunk for log retention, aggregation, consolidation, and correlation. Performance-related event analysis and monitoring are handled by PRTG and New Relic. Splunk integrates with and indexes application performance monitoring (APM) data from New Relic to provide a complete view of the platform environment.

IBM Cúram Security: The Cúram application has controls to log user activity at the table and transaction levels. Cúram also leverages other components for rule- and role-based access control (RBAC). A user who wishes to log into Cúram establishes a TLS 1.2 encrypted connection through the reverse proxy to the IBM HTTPD server front end of IBM Cúram. The encrypted connection protects the data exchange and the credentials used to establish a Cúram session.

Cúram will accept the session token that is generated at user login. Once authentication is confirmed, access to backend services, including the Oracle database, are granted and the system retrieves the user's assigned roles and application profiles. The role and application profile defined in Cúram determine what a user can see in terms of interface components, their data access, and their operations. Cúram use a lightweight directory access protocol (LDAP) directory as the repository for user IDs and passwords. This provides a central user repository to grant or revoke access and application permissions. Authentication workflows can support risk-based access control, where a workflow failure can trigger a higher-level workflow, where an additional factor is requested.

Security zone is protected by a Barracuda firewall. The zone hosts IBM Rational AppScan and a Nessus server. Each of the above zones is protected by a firewall, either a Barracuda firewall (with IDS) or an Azure NSG.

All hosts, applications, NSGs, firewall, and IDS logs are sent to Splunk for log retention, aggregation, consolidation, and correlation. Performance-related event analysis and monitoring are handled by PRTG and New Relic. Splunk integrates with and indexes application performance monitoring (APM) data from New Relic to provide a complete view of the platform environment.

IBM Cúram Security: The Cúram application has controls to log user activity at the table and transaction levels. Cúram also leverages other components for rule- and role-based access control (RBAC). A user who wishes to log into Cúram establishes a TLS 1.2 encrypted connection through the reverse proxy to the IBM HTTPD server front end of IBM Cúram. The encrypted connection protects the data exchange and the credentials used to establish a Cúram session.

Cúram will accept the session token that is generated at user login. Once authentication is confirmed, access to backend services, including the Oracle database, are granted and the system retrieves the user's assigned roles and application profiles. The role and application profile defined in Cúram determine what a user can see in terms of interface components, their data access, and their operations. Cúram use a lightweight directory access protocol (LDAP) directory as the repository for user IDs and passwords. This provides a central user repository to grant or revoke access and application permissions. Authentication workflows can support risk-based access control, where a workflow failure can trigger a higher-level workflow, where an additional factor is requested.

Security zone is protected by a Barracuda firewall. The zone hosts IBM Rational AppScan and a Nessus server. Each of the above zones is protected by a firewall, either a Barracuda firewall (with IDS) or an Azure NSG.

All hosts, applications, NSGs, firewall, and IDS logs are sent to Splunk for log retention, aggregation, consolidation, and correlation. Performance-related event analysis and monitoring are handled by PRTG and New Relic. Splunk integrates with and indexes application performance monitoring (APM) data from New Relic to provide a complete view of the platform environment.

IBM Cúram Security: The Cúram application has controls to log user activity at the table and transaction levels. Cúram also leverages other components for rule- and role-based access control (RBAC). A user who wishes to log into Cúram establishes a TLS 1.2 encrypted connection through the reverse proxy to the IBM HTTPD server front end of IBM Cúram. The encrypted connection protects the data exchange and the credentials used to establish a Cúram session.

Cúram will accept the session token that is generated at user login. Once authentication is confirmed, access to backend services, including the Oracle database, are granted and the system retrieves the user's assigned roles and application profiles. The role and application profile defined in Cúram determine what a user can see in terms of interface components, their data access, and their operations. Cúram use a lightweight directory access protocol (LDAP) directory as the repository for user IDs and passwords. This provides a central user repository to grant or revoke access and application permissions. Authentication workflows can support risk-based access control, where a workflow failure can trigger a higher-level workflow, where an additional factor is requested.

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

Security zone is protected by a Barracuda firewall. The zone hosts IBM Rational AppScan and a Nessus server. Each of the above zones is protected by a firewall, either a Barracuda firewall (with IDS) or an Azure NSG.

All hosts, applications, NSGs, firewall, and IDS logs are sent to Splunk for log retention, aggregation, consolidation, and correlation. Performance-related event analysis and monitoring are handled by PRTG and New Relic. Splunk integrates with and indexes application performance monitoring (APM) data from New Relic to provide a complete view of the platform environment.

IBM Cúram Security: The Cúram application has controls to log user activity at the table and transaction levels. Cúram also leverages other components for rule- and role-based access control (RBAC). A user who wishes to log into Cúram establishes a TLS 1.2 encrypted connection through the reverse proxy to the IBM HTTPD server front end of IBM Cúram. The encrypted connection protects the data exchange and the credentials used to establish a Cúram session.

Cúram will accept the session token that is generated at user login. Once authentication is confirmed, access to backend services, including the Oracle database, are granted and the system retrieves the user's assigned roles and application profiles. The role and application profile defined in Cúram determine what a user can see in terms of interface components, their data access, and their operations. Cúram use a lightweight directory access protocol (LDAP) directory as the repository for user IDs and passwords. This provides a central user repository to grant or revoke access and application permissions. Authentication workflows can support risk-based access control, where a workflow failure can trigger a higher-level workflow, where an additional factor is requested.

Security zone is protected by a Barracuda firewall. The zone hosts IBM Rational AppScan and a Nessus server. Each of the above zones is protected by a firewall, either a Barracuda firewall (with IDS) or an Azure NSG.

All hosts, applications, NSGs, firewall, and IDS logs are sent to Splunk for log retention, aggregation, consolidation, and correlation. Performance-related event analysis and monitoring are handled by PRTG and New Relic. Splunk integrates with and indexes application performance monitoring (APM) data from New Relic to provide a complete view of the platform environment.

IBM Cúram Security: The Cúram application has controls to log user activity at the table and transaction levels. Cúram also leverages other components for rule- and role-based access control (RBAC). A user who wishes to log into Cúram establishes a TLS 1.2 encrypted connection through the reverse proxy to the IBM HTTPD server front end of IBM Cúram. The encrypted connection protects the data exchange and the credentials used to establish a Cúram session.

Cúram will accept the session token that is generated at user login. Once authentication is confirmed, access to backend services, including the Oracle database, are granted and the system retrieves the user's assigned roles and application profiles. The role and application profile defined in Cúram determine what a user can see in terms of interface components, their data access, and their operations. Cúram use a lightweight directory access protocol (LDAP) directory as the repository for user IDs and passwords. This provides a central user repository to grant or revoke access and application permissions. Authentication workflows can support risk-based access control, where a workflow failure can trigger a higher-level workflow, where an additional factor is requested.

Security zone is protected by a Barracuda firewall. The zone hosts IBM Rational AppScan and a Nessus server. Each of the above zones is protected by a firewall, either a Barracuda firewall (with IDS) or an Azure NSG.

All hosts, applications, NSGs, firewall, and IDS logs are sent to Splunk for log retention, aggregation, consolidation, and correlation. Performance-related event analysis and monitoring are handled by PRTG and New Relic. Splunk integrates with and indexes application performance monitoring (APM) data from New Relic to provide a complete view of the platform environment.

IBM Cúram Security: The Cúram application has controls to log user activity at the table and transaction levels. Cúram also leverages other components for rule- and role-based access control (RBAC). A user who wishes to log into Cúram establishes a TLS 1.2 encrypted connection through the reverse proxy to the IBM HTTPD server front end of IBM Cúram. The encrypted connection protects the data exchange and the credentials used to establish a Cúram session.

Cúram will accept the session token that is generated at user login. Once authentication is confirmed, access to backend services, including the Oracle database, are granted and the system retrieves the user's assigned roles and application profiles. The role and application profile defined in Cúram determine what a user can see in terms of interface components, their data access, and their operations. Cúram use a lightweight directory access protocol (LDAP) directory as the repository for user IDs and passwords. This provides a central user repository to grant or revoke access and application permissions. Authentication workflows can support risk-based access control, where a workflow failure can trigger a higher-level workflow, where an additional factor is requested.

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

Security zone is protected by a Barracuda firewall. The zone hosts IBM Rational AppScan and a Nessus server. Each of the above zones is protected by a firewall, either a Barracuda firewall (with IDS) or an Azure NSG.

All hosts, applications, NSGs, firewall, and IDS logs are sent to Splunk for log retention, aggregation, consolidation, and correlation. Performance-related event analysis and monitoring are handled by PRTG and New Relic. Splunk integrates with and indexes application performance monitoring (APM) data from New Relic to provide a complete view of the platform environment.

IBM Cúram Security: The Cúram application has controls to log user activity at the table and transaction levels. Cúram also leverages other components for rule- and role-based access control (RBAC). A user who wishes to log into Cúram establishes a TLS 1.2 encrypted connection through the reverse proxy to the IBM HTTPD server front end of IBM Cúram. The encrypted connection protects the data exchange and the credentials used to establish a Cúram session.

Cúram will accept the session token that is generated at user login. Once authentication is confirmed, access to backend services, including the Oracle database, are granted and the system retrieves the user's assigned roles and application profiles. The role and application profile defined in Cúram determine what a user can see in terms of interface components, their data access, and their operations. Cúram use a lightweight directory access protocol (LDAP) directory as the repository for user IDs and passwords. This provides a central user repository to grant or revoke access and application permissions. Authentication workflows can support risk-based access control, where a workflow failure can trigger a higher-level workflow, where an additional factor is requested.

Security zone is protected by a Barracuda firewall. The zone hosts IBM Rational AppScan and a Nessus server. Each of the above zones is protected by a firewall, either a Barracuda firewall (with IDS) or an Azure NSG.

All hosts, applications, NSGs, firewall, and IDS logs are sent to Splunk for log retention, aggregation, consolidation, and correlation. Performance-related event analysis and monitoring are handled by PRTG and New Relic. Splunk integrates with and indexes application performance monitoring (APM) data from New Relic to provide a complete view of the platform environment.

IBM Cúram Security: The Cúram application has controls to log user activity at the table and transaction levels. Cúram also leverages other components for rule- and role-based access control (RBAC). A user who wishes to log into Cúram establishes a TLS 1.2 encrypted connection through the reverse proxy to the IBM HTTPD server front end of IBM Cúram. The encrypted connection protects the data exchange and the credentials used to establish a Cúram session.

Cúram will accept the session token that is generated at user login. Once authentication is confirmed, access to backend services, including the Oracle database, are granted and the system retrieves the user's assigned roles and application profiles. The role and application profile defined in Cúram determine what a user can see in terms of interface components, their data access, and their operations. Cúram use a lightweight directory access protocol (LDAP) directory as the repository for user IDs and passwords. This provides a central user repository to grant or revoke access and application permissions. Authentication workflows can support risk-based access control, where a workflow failure can trigger a higher-level workflow, where an additional factor is requested.

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

Security zone is protected by a Barracuda firewall. The zone hosts IBM Rational AppScan and a Nessus server. Each of the above zones is protected by a firewall, either a Barracuda firewall (with IDS) or an Azure NSG.

All hosts, applications, NSGs, firewall, and IDS logs are sent to Splunk for log retention, aggregation, consolidation, and correlation. Performance-related event analysis and monitoring are handled by PRTG and New Relic. Splunk integrates with and indexes application performance monitoring (APM) data from New Relic to provide a complete view of the platform environment.

IBM Cúram Security: The Cúram application has controls to log user activity at the table and transaction levels. Cúram also leverages other components for rule- and role-based access control (RBAC). A user who wishes to log into Cúram establishes a TLS 1.2 encrypted connection through the reverse proxy to the IBM HTTPD server front end of IBM Cúram. The encrypted connection protects the data exchange and the credentials used to establish a Cúram session.

Cúram will accept the session token that is generated at user login. Once authentication is confirmed, access to backend services, including the Oracle database, are granted and the system retrieves the user's assigned roles and application profiles. The role and application profile defined in Cúram determine what a user can see in terms of interface components, their data access, and their operations. Cúram use a lightweight directory access protocol (LDAP) directory as the repository for user IDs and passwords. This provides a central user repository to grant or revoke access and application permissions. Authentication workflows can support risk-based access control, where a workflow failure can trigger a higher-level workflow, where an additional factor is requested.

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

Security zone is protected by a Barracuda firewall. The zone hosts IBM Rational AppScan and a Nessus server. Each of the above zones is protected by a firewall, either a Barracuda firewall (with IDS) or an Azure NSG.

All hosts, applications, NSGs, firewall, and IDS logs are sent to Splunk for log retention, aggregation, consolidation, and correlation. Performance-related event analysis and monitoring are handled by PRTG and New Relic. Splunk integrates with and indexes application performance monitoring (APM) data from New Relic to provide a complete view of the platform environment.

IBM Cúram Security: The Cúram application has controls to log user activity at the table and transaction levels. Cúram also leverages other components for rule- and role-based access control (RBAC). A user who wishes to log into Cúram establishes a TLS 1.2 encrypted connection through the reverse proxy to the IBM HTTPD server front end of IBM Cúram. The encrypted connection protects the data exchange and the credentials used to establish a Cúram session.

Cúram will accept the session token that is generated at user login. Once authentication is confirmed, access to backend services, including the Oracle database, are granted and the system retrieves the user's assigned roles and application profiles. The role and application profile defined in Cúram determine what a user can see in terms of interface components, their data access, and their operations. Cúram use a lightweight directory access protocol (LDAP) directory as the repository for user IDs and passwords. This provides a central user repository to grant or revoke access and application permissions. Authentication workflows can support risk-based access control, where a workflow failure can trigger a higher-level workflow, where an additional factor is requested.

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

Security zone is protected by a Barracuda firewall. The zone hosts IBM Rational AppScan and a Nessus server. Each of the above zones is protected by a firewall, either a Barracuda firewall (with IDS) or an Azure NSG.

All hosts, applications, NSGs, firewall, and IDS logs are sent to Splunk for log retention, aggregation, consolidation, and correlation. Performance-related event analysis and monitoring are handled by PRTG and New Relic. Splunk integrates with and indexes application performance monitoring (APM) data from New Relic to provide a complete view of the platform environment.

IBM Cúram Security: The Cúram application has controls to log user activity at the table and transaction levels. Cúram also leverages other components for rule- and role-based access control (RBAC). A user who wishes to log into Cúram establishes a TLS 1.2 encrypted connection through the reverse proxy to the IBM HTTPD server front end of IBM Cúram. The encrypted connection protects the data exchange and the credentials used to establish a Cúram session.

Cúram will accept the session token that is generated at user login. Once authentication is confirmed, access to backend services, including the Oracle database, are granted and the system retrieves the user's assigned roles and application profiles. The role and application profile defined in Cúram determine what a user can see in terms of interface components, their data access, and their operations. Cúram use a lightweight directory access protocol (LDAP) directory as the repository for user IDs and passwords. This provides a central user repository to grant or revoke access and application permissions. Authentication workflows can support risk-based access control, where a workflow failure can trigger a higher-level workflow, where an additional factor is requested.

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

Security zone is protected by a Barracuda firewall. The zone hosts IBM Rational AppScan and a Nessus server. Each of the above zones is protected by a firewall, either a Barracuda firewall (with IDS) or an Azure NSG.

All hosts, applications, NSGs, firewall, and IDS logs are sent to Splunk for log retention, aggregation, consolidation, and correlation. Performance-related event analysis and monitoring are handled by PRTG and New Relic. Splunk integrates with and indexes application performance monitoring (APM) data from New Relic to provide a complete view of the platform environment.

IBM Cúram Security: The Cúram application has controls to log user activity at the table and transaction levels. Cúram also leverages other components for rule- and role-based access control (RBAC). A user who wishes to log into Cúram establishes a TLS 1.2 encrypted connection through the reverse proxy to the IBM HTTPD server front end of IBM Cúram. The encrypted connection protects the data exchange and the credentials used to establish a Cúram session.

Cúram will accept the session token that is generated at user login. Once authentication is confirmed, access to backend services, including the Oracle database, are granted and the system retrieves the user's assigned roles and application profiles. The role and application profile defined in Cúram determine what a user can see in terms of interface components, their data access, and their operations. Cúram use a lightweight directory access protocol (LDAP) directory as the repository for user IDs and passwords. This provides a central user repository to grant or revoke access and application permissions. Authentication workflows can support risk-based access control, where a workflow failure can trigger a higher-level workflow, where an additional factor is requested.

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

Security zone is protected by a Barracuda firewall. The zone hosts IBM Rational AppScan and a Nessus server. Each of the above zones is protected by a firewall, either a Barracuda firewall (with IDS) or an Azure NSG.

All hosts, applications, NSGs, firewall, and IDS logs are sent to Splunk for log retention, aggregation, consolidation, and correlation. Performance-related event analysis and monitoring are handled by PRTG and New Relic. Splunk integrates with and indexes application performance monitoring (APM) data from New Relic to provide a complete view of the platform environment.

IBM Cúram Security: The Cúram application has controls to log user activity at the table and transaction levels. Cúram also leverages other components for rule- and role-based access control (RBAC). A user who wishes to log into Cúram establishes a TLS 1.2 encrypted connection through the reverse proxy to the IBM HTTPD server front end of IBM Cúram. The encrypted connection protects the data exchange and the credentials used to establish a Cúram session.

Cúram will accept the session token that is generated at user login. Once authentication is confirmed, access to backend services, including the Oracle database, are granted and the system retrieves the user's assigned roles and application profiles. The role and application profile defined in Cúram determine what a user can see in terms of interface components, their data access, and their operations. Cúram use a lightweight directory access protocol (LDAP) directory as the repository for user IDs and passwords. This provides a central user repository to grant or revoke access and application permissions. Authentication workflows can support risk-based access control, where a workflow failure can trigger a higher-level workflow, where an additional factor is requested.

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

Security zone is protected by a Barracuda firewall. The zone hosts IBM Rational AppScan and a Nessus server. Each of the above zones is protected by a firewall, either a Barracuda firewall (with IDS) or an Azure NSG.

All hosts, applications, NSGs, firewall, and IDS logs are sent to Splunk for log retention, aggregation, consolidation, and correlation. Performance-related event analysis and monitoring are handled by PRTG and New Relic. Splunk integrates with and indexes application performance monitoring (APM) data from New Relic to provide a complete view of the platform environment.

IBM Cúram Security: The Cúram application has controls to log user activity at the table and transaction levels. Cúram also leverages other components for rule- and role-based access control (RBAC). A user who wishes to log into Cúram establishes a TLS 1.2 encrypted connection through the reverse proxy to the IBM HTTPD server front end of IBM Cúram. The encrypted connection protects the data exchange and the credentials used to establish a Cúram session.

Cúram will accept the session token that is generated at user login. Once authentication is confirmed, access to backend services, including the Oracle database, are granted and the system retrieves the user's assigned roles and application profiles. The role and application profile defined in Cúram determine what a user can see in terms of interface components, their data access, and their operations. Cúram use a lightweight directory access protocol (LDAP) directory as the repository for user IDs and passwords. This provides a central user repository to grant or revoke access and application permissions. Authentication workflows can support risk-based access control, where a workflow failure can trigger a higher-level workflow, where an additional factor is requested.

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

Cúram supports RBAC as well as rules where organization, location, and position have a direct impact on user access and the functions they can perform. Application profile is another user access overlay that affects what a user can see as well as how the user can interact with the system. Cúram roles and application profiles are defined to control user navigation, data access, and privileges. A requirement to restrict certain components, functions, or screens to a specific login ID can be implemented through specifically crafted roles and application profiles, which would then be assigned to the user ID. Access information is tracked through the system audit and event logs.

The PMS repository provides a secure means for authorized users to view data to which they have been granted access. Connections to the PMS data repository are encrypted using TLS 1.2. Data are encrypted at rest using Federal Information Processing Standard (FIPS) 140-2–validated cryptographic modules. The federal government's standard for encryption requires the use of cryptographic modules that have been through the NIST FIPS 140-2 validation process to ensure that products are using strong, vetted encryption. Authentication occurs against an LDAP directory and two-factor authentication is required by system, network, and database administrators before being granted access to the system environment. RBAC is used to determine a user's privileges within the system environment. User accounts and assigned roles are approved before the user account is created and are reviewed and certified on a periodic basis.

We apply the principle of least privilege to role definition and role assignment. Users are not granted access to data or functions they do not need as part of their job duties. We implement the separation of duties principle through careful role assignment and the periodic reassessment of assigned roles (typically every 90 or 180 days, depending on the data sensitivity). Roles are assigned in a way where an employee does not have full access to the functions performed as part of a process. If an employee can change assigned security roles or role definitions, they do not have maintenance or archiving privileges on the logging and monitoring infrastructure.

The IBM Cúram system includes an internal secure message interface. Email notifications are sent to providers when a new message has arrived in their Cúram message inbox. The message interface gives providers the ability to respond to the messages they have received. Cúram generates an audit trail at the table and business transaction levels containing information on who made the change and when it was made. This audit trail can review user, business process, and workflow activity for anomalous behavior. Audit trails will be integrated with Splunk which will operate as a single repository for security audit and investigations. The solution will be sized to meet the auditing requirements and maintain system performance SLAs.

Team NewWave's proposed PMS will include a Secure FTP server. Connections to the Secure FTP servers are encrypted using FIPS 140-2–validated cryptographic algorithms. Data files uploaded to the Secure FTP server are written to a directory structure that is encrypted at rest using FIPS 140-2–validated cryptographic algorithm. The directory structure folders are polled by IBM Integration Broker (IIB) to identify when files are available for processing. Before attempting any operations on the file, a check is performed to confirm upload operations have finished writing the file to disk. The polling interval time is configurable. The Secure FTP server can make files available to the state and state-approved trading partners.

We perform active monitoring to detect anomalous activities. Security events are generated for role assignments. Privileged role assignments require additional authorization levels and trigger notifications on assignment. Data access and exports are logged and reviewed periodically during post-incident analysis.

Other Security Considerations: Team NewWave creates offline or redundant backups to mitigate the risk of a ransomware attack or other malicious activity on the system by a user, virus, worm, or other type of malware. These backups are encrypted at rest within MAG data centers. Keys are stored in an encrypted Key Vault. Access to offline data requires multifactor authentication by authorized users, along with permissions to the Key Vault and underlying encrypted data.

Team NewWave has designed the system architecture to include active and passive failover support for disaster recovery (DR). The architecture also includes load balancers and redundant components for high availability and performance reasons but can trigger a failover to the disaster recovery location leveraging the instances that have been created in the alternate environment. The geo-redundant storage automatically replicates to the alternate region and the Oracle database synchronization capability supports having a copy of the database in the alternate processing environment.

Team NewWave will plan, schedule, and circulate contingency plan (CP) and DR test scenarios for review and feedback and will then conduct annual (at a minimum) CP and DR exercises coordinated with state calendar activities and resources. Team NewWave will use guidance provided by the state and CMS as well as NIST SP 800-34 revision 1 *Contingency Planning Guide for Federal Information Systems.*

Team NewWave has implemented several strategies in the system design that align with the NIST Cyber Security Framework. The system controls and architecture are designed to identify, protect, detect, respond to, and recover from attacks and system

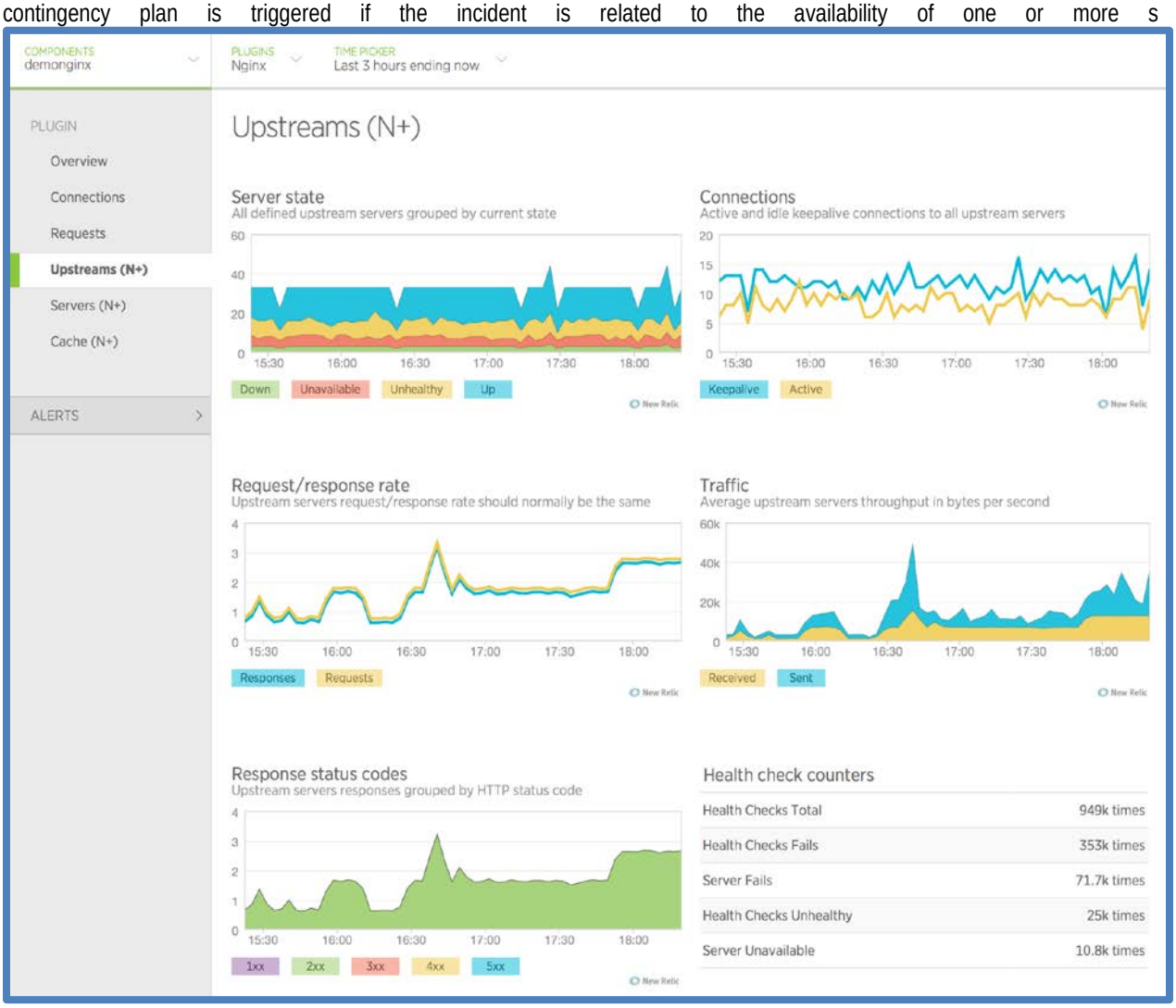
Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

availability issues. Team NewWave will provide a system availability report that identifies any unplanned outages as well as whether or not the system availability threshold of 99.5% was met. The report will also identify planned maintenance windows that have been approved by the state to verify whether or not maintenance resulted in periods of downtime longer than the standard 4- to 8-hour window. The state may decide to approve longer maintenance windows if it agrees with Team NewWave that the maintenance is required. New Relic assists in system response time monitoring to ensure 99.5% of user system interactions receive a response in less than 2 seconds (or less than 4 seconds from the TMMIS firewall).

New Relic Portal: New Relic is an application performance management system that captures detailed metrics for each transaction, including time spent in each component, database queries, external API calls, and so on. New Relic Real-User Monitoring embeds JavaScript code into the user's browser to capture end-user performance experience. When the page is rendered in the browser, the New Relic beacon gets a request providing performance metrics on the back-end, network, Document Object Model (DOM) processing, and page rendering times. Systems engineers can use the information to identify bottlenecks, slow-running queries, system errors, and other actionable events. The fact that the metrics are captured in each component as well as in the end user's browser provides evidence-based data related to system performance. For example, if a user's browser takes a long time to render the web page, the metrics will reflect that. If a local ISP or an ISP along the path experiences routing or network congestion issues, the data will reflect that issue. Slow database queries due to a missing or corrupted index resulting in full table scans will be identified in the New Relic portal.

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

The notification process includes periodic reports delivered to the state to provide trended metrics related to application performance and accessibility. Notifications also occur from triggering a notification based on criteria identified in the incident response, CP, DR, or continuity of operations plans. The state is notified of any known or suspected security or privacy event within 1 hour of detection. Team NewWave follows this approach to apprise the state of potential issues that warrant attention. An event does not become an incident until enough information is collected to confirm that it is an actual security or privacy incident. On further investigation, if the suspected incident is a false positive, a communication is sent to state-designated personnel to report the false positive and close out the incident. If it is an actual incident, an incident report containing the timeline of the incident, actions taken, root cause analysis, and corrective action plan is sent to the state within 12 hours. The contingency plan is triggered if the incident is related to the availability of one or more s



ystem components. If an entire data center or region becomes unavailable, the DR plan may be triggered to begin the recovery process at the alternate processing site. If an environmental event affects the location where state or contractor employees conduct their daily work, the continuity of operations plan may be triggered. Each plan type includes a process, call tree, potential triggering events, and activation criteria.

Figure 8: New Relic Portal Screen Shot

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

Team NewWave has held CMS contracts for hosted systems since 2008; we are familiar with NIST, HIPAA, and CMS requirements. We also assist states and CMS as the T-MSIS contractor. Throughout the implementation and operation of the PMS, we will implement and maintain the models, guidelines, and principles that make up the Medicaid Information Technology Architecture (MITA) 3.0 Framework as approved by the state. From a security architecture perspective, we will meet or exceed system-level goals outlined in the MITA based on Health and Human Services Commission (HHSC) decisions and product capability, including implementation of SSO (for possible planned integration with the enterprise SSO initiative, aka ESSO, but initially as SSO within the PMS environment). We will implement and maintain National Health Information Technology application or solution architecture principles.

The COTS product, IBM Cúram, forms the core of the PMS environment. This system has been implemented successfully as part of provider enrollment management systems in other states. The overall system conforms to the goals and architecture as defined under the umbrella of the Federal Health Architecture (FHA), which includes the National Health Information Technology principles and compliance with the Federal Enterprise Architecture (FEA).

Cúram supports the 2017 Interoperability Standards Advisory: Office of the National Coordinator for Health IT (the ISA) as defined in section I-E: Health Care Providers.

The two standards listed under interoperability need, representing healthcare providers, are as follows:

- National Provider Identifier (NPI)
- National Uniform Claim Committee (NUCC).

All system interfaces between PMS and other healthcare ecosystem components will be performed over encrypted communication channels using FIPS 140-2–validated cryptographic modules. In most cases, TLS 1.2 is used to support HTTPS encrypted communications. In some cases, IPSec VPN tunnels may be implemented between two system components communicating across an untrusted medium such as the Internet. Email servers will be configured to force server-to-server TLS encryption for known partners in accordance with CMS' Business Partner System Security Manual (BPSSM).

The BPSSM is a mitigating control that serves to protect unencrypted emails sent to intended recipients over the Internet. Team NewWave staff have received training and know how to encrypt email containing PII, PHI, or FTI data. Encryption is implemented in one of two ways by Team NewWave, as follows:

- The Office 365 subscription for Team NewWave is configured to encrypt emails when the keyword *encrypted* is present in the subject line.
- If a file attachment in the email needs to be encrypted, but the email itself does not, SecureZIP with FIPS mode enabled can be used to encrypt, compress, and password-protect the email attachment. Passwords for the attachment are communicated out-of-band, such as by phone.

A.27 DOCUMENTATION

Documentation: Team NewWave will provide all required documentation following industry best practices using our library of templates and processes from NewWave's CCMI Level 4 Services–appraised Process Asset Library. These documentation templates cover all project management disciplines, as described in CMMI, PMBOK, ITIL, CMS XLC and from our experience in systems development, integration, implementation, operations, and security. Our document deliverables will be tailored for PMS and approved by AHCCCS/Med-QUEST.

In addition to the PMP and subordinate management plans, we will deliver other major deliverables, such as PMS System Design Document (SDD), Interface Control Document (ICD), and operations, functional, and user documentation, to AHCCCS/Med-QUEST for approval. We will track all deliverables and their due dates in the PWP. Our deliverables and documentation (in addition to our software modules) will fall under our proposed Configuration Management and Configuration Control Board processes described in our Configuration Management Plan (CMP). See our PMP in Appendix B for additional information on our CMP. All approved changes to the Provider Management System or its environments will be reflected in updated in the appropriate documentation within 10 days of taking affect.

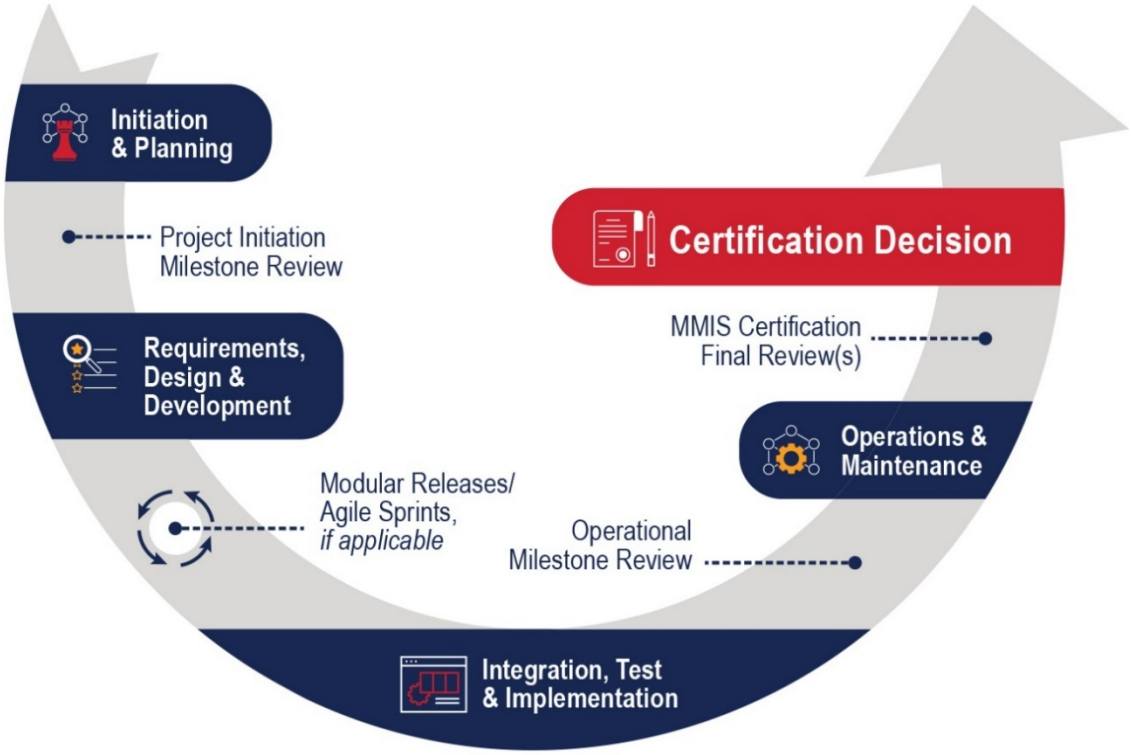
Team NewWave will use SharePoint to provide a repository and project portal. The SharePoint site will be accessible by all Team NewWave members and PMS stakeholders, as approved by state decision makers.

CMS Certification: Team NewWave will actively support AHCCCS/Med-QUEST preparation for the CMS certification review, and we will be available to assist during the CMS onsite review. Our proposed IBM Cúram product has been approved for continued federal funding within a currently certified MMIS in multiple states, including California, Georgia, Illinois, Indiana, Kansas, Michigan, Mississippi, Montana, Nebraska, New Jersey, New York, North Dakota, Ohio, and South Carolina. As a trusted Medicaid partner who is well known to CMS, our team has experience in helping our clients throughout the certification

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

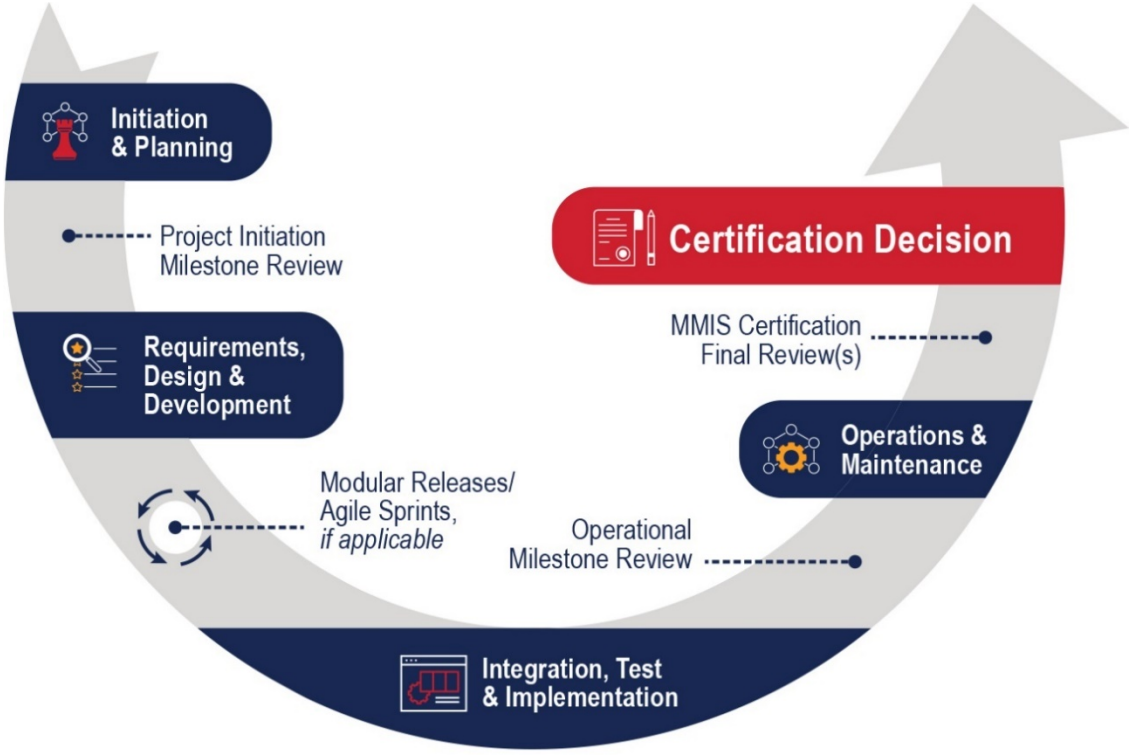
process. We have identified Ms. Sherry Travis as our CMS Certification SME who will be able to assist AHCCCS/Med-QUEST as you go through the CMS certification process.

We will work with AHCCCS/Med-QUEST and the IV&V contractor to support CMS certification as needed, starting early during the requirements and preliminary design phase. We will dedicate two resources—NewWave Operations Manager and Business Analyst Lead—to ensure planning and the collection of required artifacts and activities from contract start until AHCCCS/Med-QUEST receives CMS certification.



We will develop and submit to AHCCCS/Med-QUEST our CMS Certification Plan, which documents a systematic approach and

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.



methodology for obtaining certification of the AHCCCS/Med-QUEST PMS. The CMS Certification Plan will be incorporated and tracked in the Project Plan, reflecting processes we have integrated with project management disciplines and associated plans. We will incorporate milestones and Critical Success Factors into our system certification plan. We will develop our plan by creating a single plan from the following four separately approved milestone plans:

- Project Management Plans
- MITA documents
- MMIS concept of operations
- Planning Advance Planning Document (PAPD) and Implementation Advance Planning Document (IAPD)

We incorporate the Medicaid Enterprise Certification Toolkit (MECT) Provider Management Checklists from the beginning of requirements and design through User Acceptance Testing (UAT) and Operational Milestone Reviews. We generate or collect the artifacts for satisfying the 44 System Review Criteria in the checklist following the Medicaid Enterprise Certification Life Cycle (MECL) certification steps, as depicted in Figure 10. We also will be available during the actual CMS onsite review to assist with any CMS follow-up requests.

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

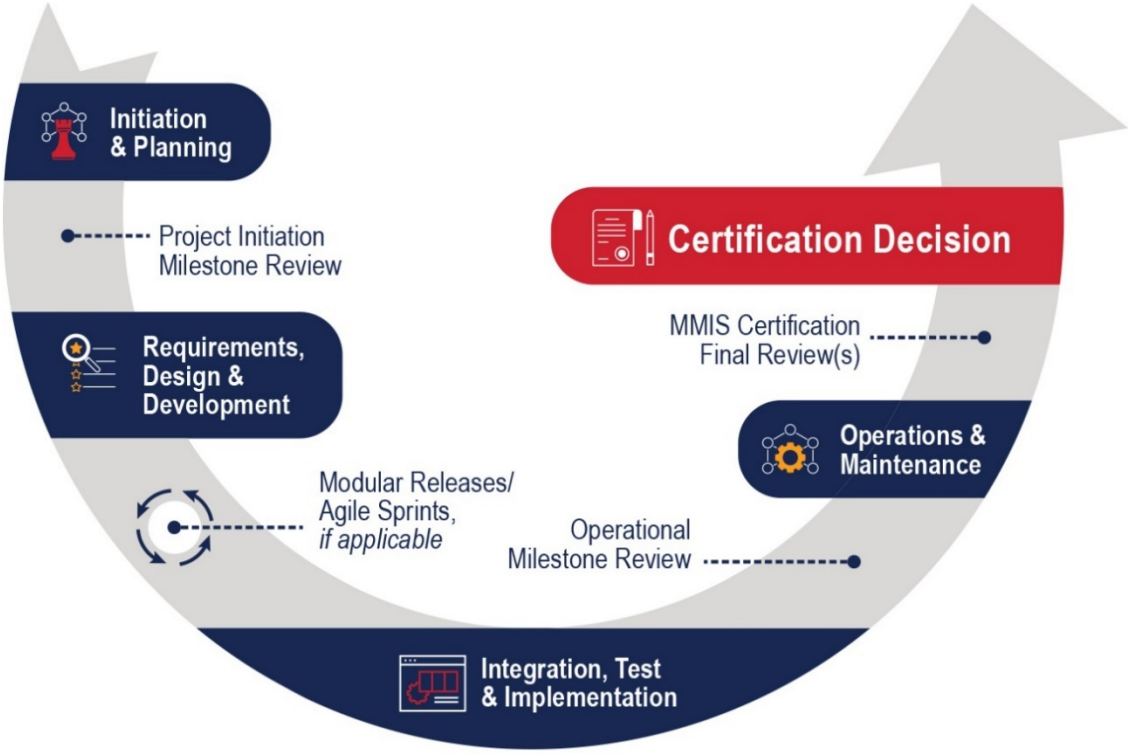


Figure 9: MECL Module Certification Steps

Early in the project plan execution, we will develop and submit our CMS Certification Management Plan. This document includes the following topics: Purpose and Scope; CMS Medicaid Enterprise Certification Toolkit (MECT); Certification Reporting; MITA; Roles and Responsibilities; Integration with Registration & Attestation System Implementation; and CMS Certification Process. We will walk through the schedule with you, obtain your approval, and continue to maintain the schedule, making changes at your direction. We will ensure that all artifacts and deliverables listed in the schedule arrive complete and on time and will assist AHCCCS/Med-QUEST in preparing the CMS Certification Review Package. As mentioned above, we will apply our experience on other successful CMS certifications to ensure your certification proceeds as efficiently as possible.

Certification Progress Reviews: Certification progress reviews are conducted with NewWave, AHCCCS/Med-QUEST, and CMS. Preparation for the CMS site visit is supported by planning and preparatory meetings during the implementation process.

Post-Implementation CMS Readiness Review: A Post-Implementation Readiness Review schedule for final certification preparation is developed during implementation and used to manage post-implementation activities. We will work with AHCCCS/Med-QUEST to understand the CMS Certification Readiness Review schedule for the required planning, preparation, and certification activities. We will walk through the review plan and schedule to ensure all reports and other deliverables listed in the readiness review arrive complete and on time, and we will help prepare the CMS Certification Review Package.

Team NewWave will maintain staffing continuity for the various business and technical operations throughout completion of all certification activities. When required, we will organize onsite (or remote) follow-up discussions to resolve compliance issues related to the federal certification process.

A.28 Knowledge Transfer

Our commitment to knowledge transfer is guided in large part by collaboration between Arizona, Hawaii, and Team NewWave, which will result in a well-executed training plan that includes knowledge transfer. This is the basis for how we are collectively committed to delivery, execution, and outcomes for AHCCCS/Med-QUEST and the user experience. We will have specific timelines, durations, and curriculums with respect to tools, data, and desired outcomes, ensuring that timely and comprehensive

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

knowledge transfer occurs. We will have knowledge transfer measured by surveys and testing. See Section A.19 for details on our training approach.

A.29 Cultural Change Management and Communication

In responding to this section, Team NewWave describes our approach for a change in culture and in change management. We understand the impact on an organization's culture and rhythm when upgrading multiple systems of record to a streamlined, online, data-driven business syst

A.30 Deployment and Roll Out Support

Team member IBM Watson Health has experience in implementing, deploying, and supporting complex systems for multiple government agencies. In the past 10 years, IBM Cúram has been implemented in more than 10 states, with multiple implementations in California and New York and in New York City. We tailored our proven Agile Development Methodology (ADM) to provide the best opportunity to

A.30 Deployment and Roll Out Support

Team member IBM Watson Health has experience in implementing, deploying, and supporting complex systems for multiple government agencies. In the past 10 years, IBM Cúram has been implemented in more than 10 states, with multiple implementations in California and New York and in New York City. We tailored our proven Agile Development Methodology (ADM) to provide the best opportunity to complete the implementation of our proposed solution within the 9-month window required by AHCCCS/Med-QUEST.

Our ADM encourages a flexible and decentralized approach to software delivery in which team members respond to changing environments through continuous feedback and collaboration. Transparency through continuous feedback, along with continuous integration and automation, is key to quality software implementation. See our proposed PMP in Appendix B for details of our Deployment Plan.

For rollout support, Team NewWave's release and deployment management approach ensures that the pre-built, packaged components delivered contain all the necessary modules and are evaluated by schedule, risk, and urgency by the Change Control Board. Our processes ensure that packages are versioned, baselined, and placed in position to be leveraged by the Cúram automated build and deployment tools. Our team ensures that packages are validated (see Section A.20 Testing) before deployment to ensure the quality and effectiveness of the automated deployments. These packages will be the baseline packages for release in the various testing environments, ensuring consistency in the lifecycle environments.

The disciplined and automated promotion of the packages through the non-production environments, always before introduction to the production environment, provides multiple quality gates before making any changes in production that may affect system availability or end-user satisfaction. We also use automated post-installation *smoke* tests to rapidly evaluate the effectiveness of deployments and verify key functionality within the applications in production.

complete the implementation of our proposed solution within the 9-month window required by AHCCCS/Med-QUEST.

Our ADM encourages a flexible and decentralized approach to software delivery in which team members respond to changing environments through continuous feedback and collaboration. Transparency through continuous feedback, along with continuous integration and automation, is key to quality software implementation. See our proposed PMP in Appendix B for details of our Deployment Plan.

For rollout support, Team NewWave's release and deployment management approach ensures that the pre-built, packaged components delivered contain all the necessary modules and are evaluated by schedule, risk, and urgency by the Change Control Board. Our processes ensure that packages are versioned, baselined, and placed in position to be leveraged by the Cúram automated build and deployment tools. Our team ensures that packages are validated (see Section A.20 Testing) before deployment to ensure the quality and effectiveness of the automated deployments. These packages will be the baseline packages for release in the various testing environments, ensuring consistency in the lifecycle environments.

The disciplined and automated promotion of the packages through the non-production environments, always before introduction to the production environment, provides multiple quality gates before making any changes in production that may affect system availability or end-user satisfaction. We also use automated post-installation *smoke* tests to rapidly evaluate the effectiveness of deployments and verify key functionality within the applications in production.

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

em in IBM's Cúram product. We view our relationship with our customers as a partnership working toward a common goal of improving and streamlining the providers' and states' experience in meeting federal and state requirements for managed care programs.

Our experienced management team, business analysts, and training manager will create an educational training program for AHCCCS/Med-QUEST trainers to provide all users of the new PMS. We will also provide status updates that can be communicated across the user base to increase awareness of the changes to day-to-day activities in performing work under the new PMS. See Section A.19 on Training for details. Team NewWave also will develop a Communications Plan as described in our draft PMP in Appendix B.

Team NewWave knows the complexities and challenges associated with change management across a large implementation and operational environment. To meet the needs of the AHCCCS/Med-QUEST PMS contract, we will ensure that through the administration of the AHCCCS/Med-QUEST, all changes to documentation, systems software, and data stores are evaluated, prioritized, coordinated, documented, and monitored.

Team NewWave provides change management services consistent with ITIL, CMMI, and the federally authorized CMS XLC, which includes adherence to change management processes and implementation, customization, administration, enhancement, and use of processes and tools. We describe our change management process in the Configuration Management section of our PMP in Appendix B.

Team NewWave follows our mature risk management and tailored communication and change management processes to ensure successful migrations. Our Quality Management Plan describes the quality checks and metrics we propose to gather, analyze, and report, as follows:

- Ensure that change requests, problem reports, engineering change proposals, and deployment requests are processed, evaluated, and adjudicated in a timely manner.
- Evaluate scope, applicability, and the effect of changes, focusing on cost, schedules, and compliance with security or technical requirements.
- Provide approval or disapproval based on risk, defined strategic initiatives, program business objectives, and budgetary parameters.

A.30 Deployment and Roll Out Support

Team member IBM Watson Health has experience in implementing, deploying, and supporting complex systems for multiple government agencies. In the past 10 years, IBM Cúram has been implemented in more than 10 states, with multiple implementations in California and New York and in New York City. We tailored our proven Agile Development Methodology (ADM) to provide the best opportunity to complete the implementation of our proposed solution within the 9-month window required by AHCCCS/Med-QUEST.

Our ADM encourages a flexible and decentralized approach to software delivery in which team members respond to changing environments through continuous feedback and collaboration. Transparency through continuous feedback, along with continuous integration and automation, is key to quality software implementation. See our proposed PMP in Appendix B for details of our Deployment Plan.

For rollout support, Team NewWave's release and deployment management approach ensures that the pre-built, packaged components delivered contain all the necessary modules and are evaluated by schedule, risk, and urgency by the Change Control Board. Our processes ensure that packages are versioned, baselined, and placed in position to be leveraged by the Cúram automated build and deployment tools. Our team ensures that packages are validated (see Section A.20 Testing) before deployment to ensure the quality and effectiveness of the automated deployments. These packages will be the baseline packages for release in the various testing environments, ensuring consistency in the lifecycle environments.

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

THE DISCIPLINED AND AUTOMATED PROMOTION OF THE PACKAGES THROUGH THE NON-PRODUCTION ENVIRONMENTS, ALWAYS BEFORE INTRODUCTION TO THE PRODUCTION ENVIRONMENT, PROVIDES MULTIPLE QUALITY GATES BEFORE MAKING ANY CHANGES IN PRODUCTION THAT MAY AFFECT SYSTEM AVAILABILITY OR END-USER SATISFACTION. WE ALSO USE AUTOMATED POST-INSTALLATION *SMOKE* TESTS TO RAPIDLY EVALUATE THE EFFECTIVENESS OF DEPLOYMENTS AND VERIFY KEY FUNCTIONALITY WITHIN THE APPLICATIONS IN PRODUCTION. A.30 DEPLOYMENT AND ROLL OUT SUPPORT

Team member IBM Watson Health has experience in implementing, deploying, and supporting complex systems for multiple government agencies. In the past 10 years, IBM Cúram has been implemented in more than 10 states, with multiple implementations in California and New York and in New York City. We tailored our proven Agile Development Methodology (ADM) to provide the best opportunity to complete the implementation of our proposed solution within the 9-month window required by AHCCCS/Med-QUEST.

Our ADM encourages a flexible and decentralized approach to software delivery in which team members respond to changing environments through continuous feedback and collaboration. Transparency through continuous feedback, along with continuous integration and automation, is key to quality software implementation. See our proposed PMP in Appendix B for details of our Deployment Plan.

For rollout support, Team NewWave's release and deployment management approach ensures that the pre-built, packaged components delivered contain all the necessary modules and are evaluated by schedule, risk, and urgency by the Change Control Board. Our processes ensure that packages are versioned, baselined, and placed in position to be leveraged by the Cúram automated build and deployment tools. Our team ensures that packages are validated (see Section A.20 Testing) before deployment to ensure the quality and effectiveness of the automated deployments. These packages will be the baseline packages for release in the various testing environments, ensuring consistency in the lifecycle environments.

The disciplined and automated promotion of the packages through the non-production environments, always before introduction to the production environment, provides multiple quality gates before making any changes in production that may affect system availability or end-user satisfaction. We also use automated post-installation *smoke* tests to rapidly evaluate the effectiveness of deployments and verify key functionality within the applications in production.

A.30 DEPLOYMENT AND ROLL OUT SUPPORT

Team member IBM Watson Health has experience in implementing, deploying, and supporting complex systems for multiple government agencies. In the past 10 years, IBM Cúram has been implemented in more than 10 states, with multiple implementations in California and New York and in New York City. We tailored our proven Agile Development Methodology (ADM) to provide the best opportunity to complete the implementation of our proposed solution within the 9-month window required by AHCCCS/Med-QUEST.

Our ADM encourages a flexible and decentralized approach to software delivery in which team members respond to changing environments through continuous feedback and collaboration. Transparency through continuous feedback, along with continuous integration and automation, is key to quality software implementation. See our proposed PMP in Appendix B for details of our Deployment Plan.

For rollout support, Team NewWave's release and deployment management approach ensures that the pre-built, packaged components delivered contain all the necessary modules and are evaluated by schedule, risk, and urgency by the Change Control Board. Our processes ensure that packages are versioned, baselined, and placed in position to be leveraged by the Cúram automated build and deployment tools. Our team ensures that packages are validated (see Section A.20 Testing) before deployment to ensure the quality and effectiveness of the automated deployments. These packages will be the baseline packages for release in the various testing environments, ensuring consistency in the lifecycle environments.

The disciplined and automated promotion of the packages through the non-production environments, always before introduction to the production environment, provides multiple quality gates before making any changes in production that may affect system availability or end-user satisfaction. We also use automated post-installation *smoke* tests to rapidly evaluate the effectiveness of deployments and verify key functionality within the applications in production.

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

A.31 Production Transfer

Team NewWave will deliver an Operational Readiness Review (ORR) Plan at least 8 weeks before the agreed-on project go-live date for AHCCCS/Med-QUEST approval. Team NewWave has successfully passed ORRs for many states and for CMS and will apply lessons learned to AHCCCS/Med-QUEST implementations (see our Past Performance references). This ORR Plan describes our approach to transition the PMS into production and describes the environment (people, processes, and technology) and responsibilities, risks, and assumptions. The ORR must begin at least 4 weeks before the agreed-on project go-live date. AHCCCS/Med-QUEST approval to proceed is obtained 2 weeks before the designated go-live date.

The ORR is approved based on the following assumptions:

1. Azure Cloud Hosting PROD environment has been reviewed and approved by the state. This may include a site visit to the facility.
2. Review of defect log and understanding of any defects identified as high, along with a mitigation plan.
3. UAT has been completed and no showstoppers exist.
4. All security requirements have been met and have been approved by the state.
5. Enrollment functionality (add references from SOW) is implemented per requirements.
6. On-Line Provider Directory (add references from SOW) is implemented per requirements.
7. Reporting and reports (add references from SOW) are implemented per requirements.
8. Interfaces (add references from SOW) are implemented per requirements.
9. Data conversion (add references from SOW) has been successfully tested.

Team NewWave will provide our plan for supporting the production go-live date at least 2 weeks before the ORR for AHCCCS/Med-QUEST review and approval.

A.32 Post-Implementation Support

Team NewWave has several federal and state systems we operate and maintain in production environments (see Past Performance references). We typically arrange our post-implementation support into three tiers, as described below. Beyond the application architecture, which is designed to be fault tolerant, we maintain and configure changes as required. Team NewWave scans the environment to ensure each component is functioning correctly and sends alerts when we identify issues. When issues are identified, we mitigate their business impact and ensure the PMS environment is performing per the required SLAs.

Team NewWave is adaptive, enabling us to respond to requested changes quickly and in accordance with our state-approved Configuration Management Plan. We find and correct system issues with minimum downtime and we schedule all maintenance requirements during the standard, state-approved maintenance window to minimize impact on business operations. Team NewWave follows ITIL and CMMI best practices to improve user experience, system support, and application performance.

Levels of Support Offered: During implementation, Team NewWave will engage with AHCCCS/Med-QUEST to ensure appropriate communication processes are in place to support a timely response to reported tickets. We also work with contract representatives to ensure appropriate support teams are assigned tickets, in turn ensuring a timely response to tickets. Our three tiers of support are Systems Support, Electronic Information Transmission Support, and Network Support.

Systems Support

- Level 1: As a basic level of support, we triage, troubleshoot, and resolve basic problems. Examples include answering basic how-to questions, resetting passwords, creating accounts, and so on. The engineer (or user) creates a ticket to annotate the work performed and to escalate, if necessary.
- Level 2: For issues that cannot be resolved by the first level of support, we call on a support team with in-depth knowledge of the various systems and components to investigate, identify, and resolve the issue. We report major issues and communicate the mitigation plan to the end user.
- Level 3: All systems maintenance and support is handled proactively. Systems are monitored 24x7 with in-depth application monitoring and testing to ensure each component is functioning properly. A team is assigned revolving maintenance tasks to ensure services are up-to-date and compliant with all security requirements. The updates are planned, scheduled, and tested before implementation into the production environment. All changes are approved by a Change Control Board.

Electronic Information Transmission Support

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

- Level 1: The PMS has interfaces with other state and federal systems; thus, a support team addresses any specific issues with data transfer. The support engineer determines if there is an issue with sending or receiving data, or with the data itself. The engineer then contacts the appropriate department to address any issues with data transfer. The specific department documents the user's issues in the ticketing system and ensures a resolution is communicated to the customer.
- Level 2: We escalate any issues that cannot be resolved by the primary support engineer. The escalation engineer troubleshoots system issues, including database or networking issues that prevent data transfer.

Network Support

- Level 1: The networking team ensure that each component has network connectivity and that traffic is balanced across servers and firewalls. It monitors and works with other teams to ensure 100% uptime, and proactively reviews logs to ensure there has been no security breach.
- Level 2: All interconnectivity and exchange of data is handled by an advanced group of network engineers who set up data transfers and troubleshoot issues that arise.

Database Support: A team of database engineers maintain the data integrity in the PMS. They ensure that all transactions are backed up and that data remain consistent. They ensure all data transfers are formatted, scheduled, and that data are ingested correctly.

Process for Requesting Support: The AHCCCS/Med-QUEST Contact Centers initiate service requests. Team NewWave requires access to their ticketing applications to close tickets. We use Jira to track PMS environment tickets, ensuring we have full visibility into system support activities. We assign severity levels to tickets for agreed-on SLAs, or as prioritized by the Change Control Board.

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

APPENDIX A: CÚRAM SCREEN SHOTS

To enhance the reader experience, supplement our responses to requirements and to help the reader visualize the look and feel of the proposed PMS User Interface, we are presenting a sample set of screen shots. Introductions to the screen shots are brief however, we have provided requirements numbers directing you to the specific requirement and our response to that requirement.

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

Provider Enrollment Process

The PMS will support the provider enrollment process. Providers will be guided through this process using a workflow configured to support the State's provider enrollment process as discussed in Requirement 5.1.2.

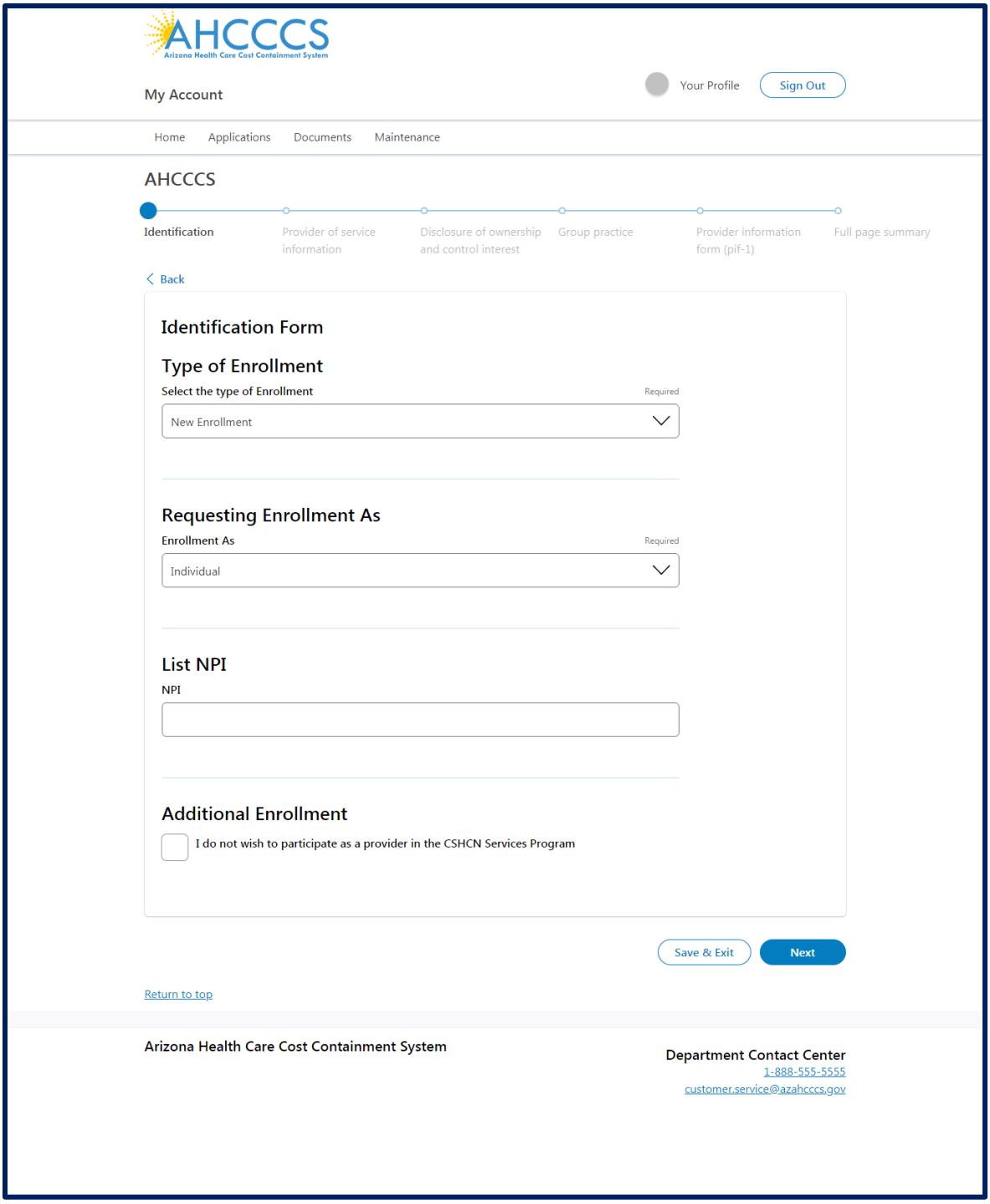


Figure 10: Guided Process for Provider Enrollment

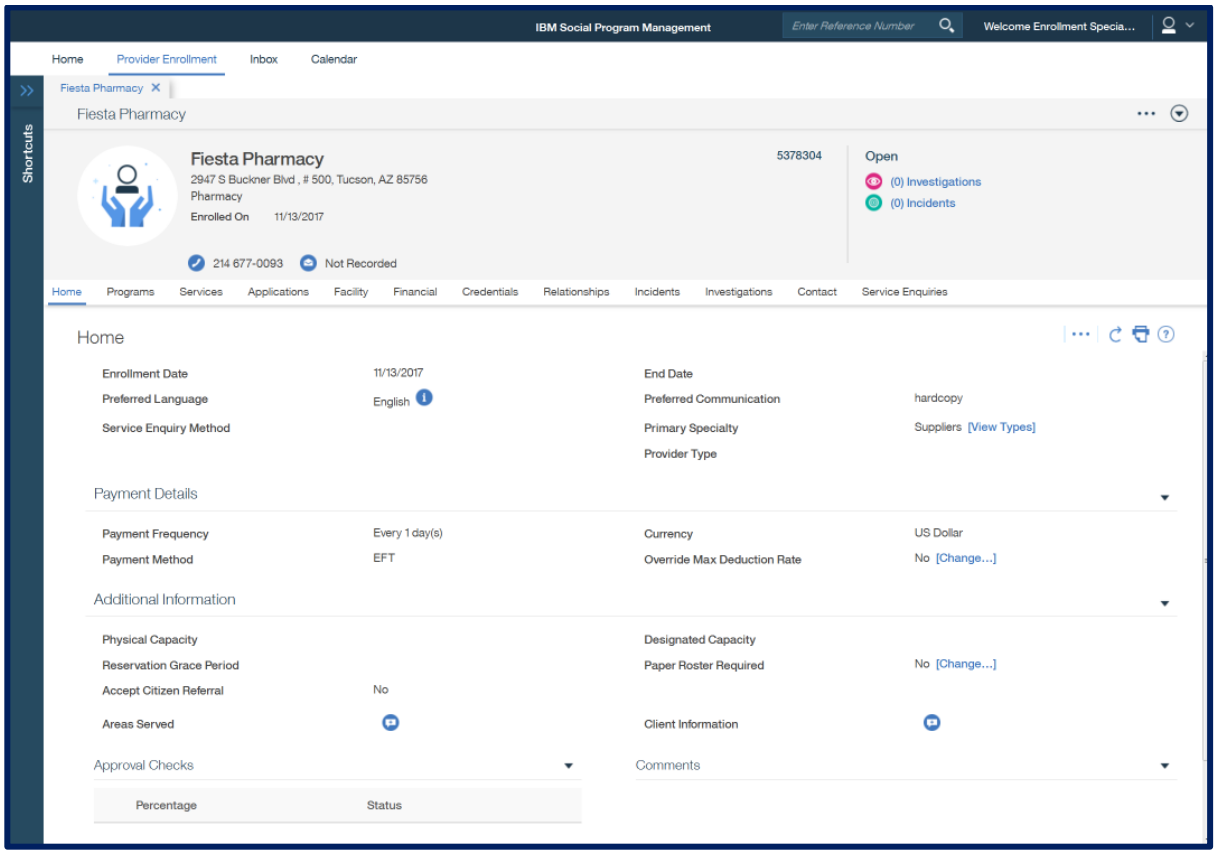
Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

Provider Home Page

The PMS is designed to track provider details including facilities, service locations, provider credentials, and ownership. The Provider Home Page displace provider details, as discussed in Requirement 5.1.3.

Figure 11: Provider Home Page

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.



Provider Enrollment – Required Documentation

The PMS will support the provider enrollment process tracking verifications and documentations required to process the provider's enrollment request. The PMS will provide a list of documents required and maintain a list of provided and outstanding documents as displayed in the screen shot below. This is further discussed in Requirement 5.1.6.

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

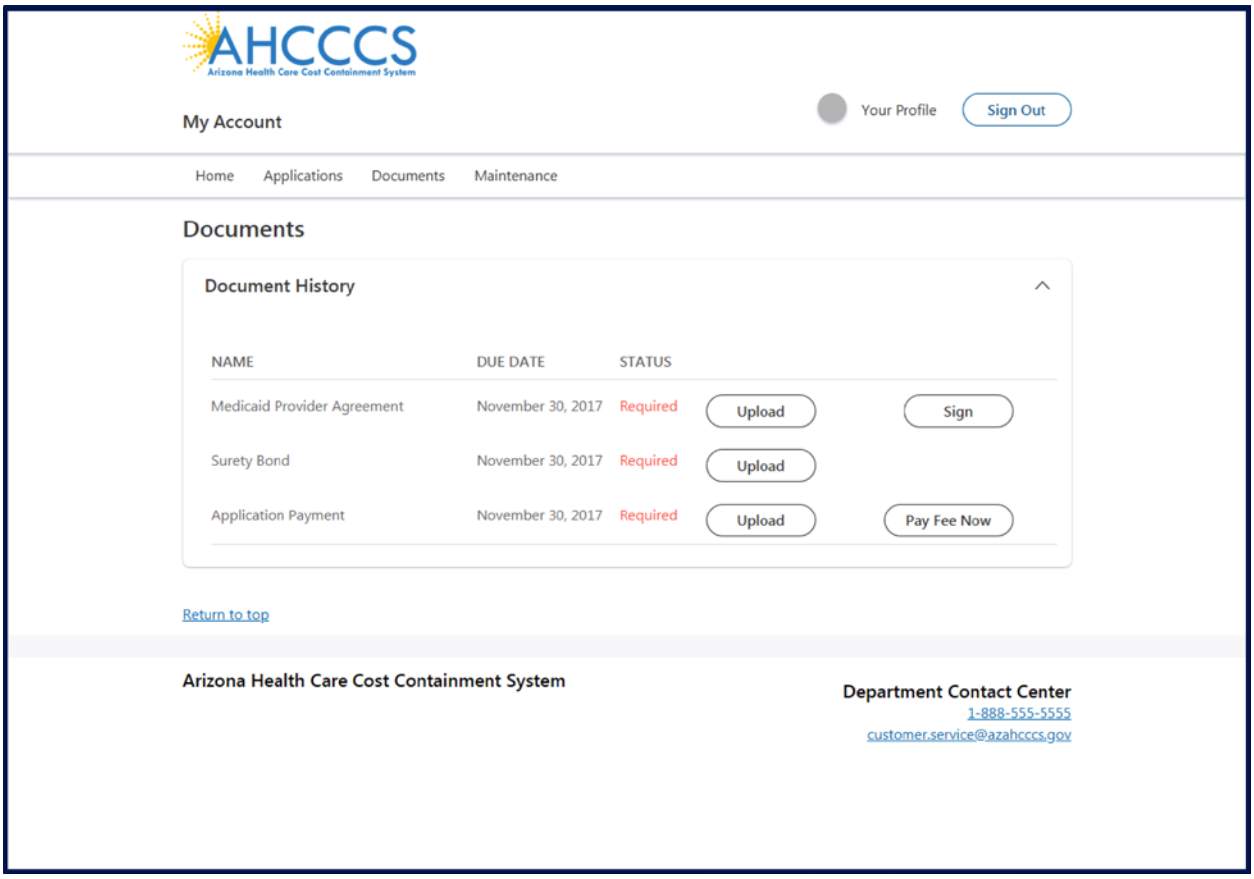


Figure 12: Provider Enrollment – required documentation

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

Enrollment Specialist Dashboard:

Upon logging into the PMS, users are directed to their home page. This sample Enrollment Specialist Dashboard is discussed in Requirement 5.1.14

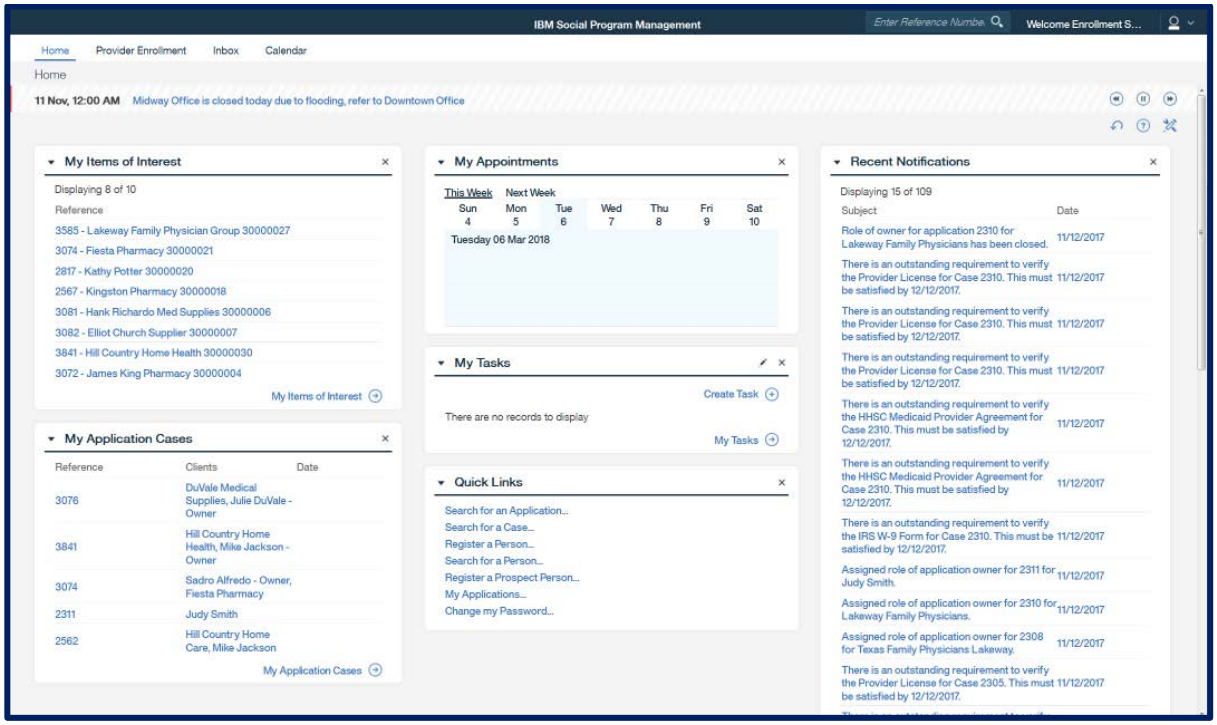


Figure 13: Enrollment Specialist Dashboard

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

Provider Portal Home Page

Upon logging into the PMS, providers are directed to their home page. This sample Provider Portal Home Page discussed in Requirement 5.1.14.

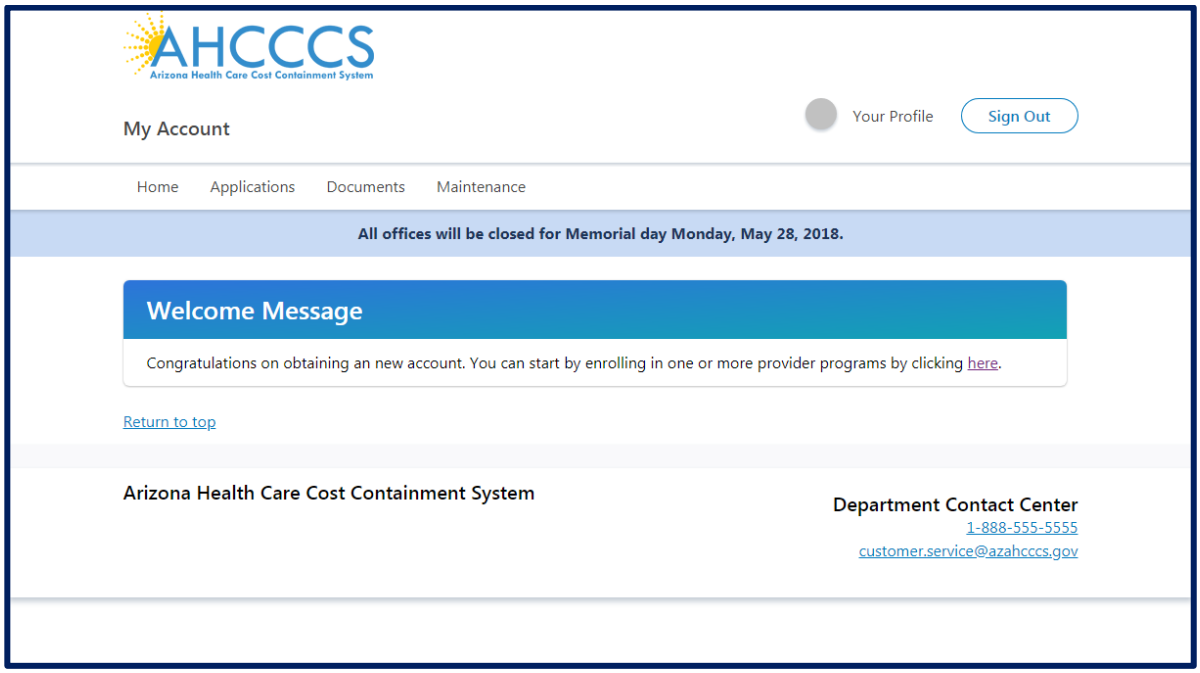


Figure 14: Provider Portal Home Page

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

Application Evidence Dashboard:

The information collected throughout the enrollment process will be mapped to the application. The Application Evidence Dashboard, as discussed in Requirement 5.5.5, will provide the status of information and required verifications.

Figure 15: Application Evidence Dashboard

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

Application Verifications

The Application process will check for duplicates and determine the outstanding items or documents required to process the provider's application. The Application Verification view displays the list of verifications on an application, as discussed in Requirement 5.5.6.

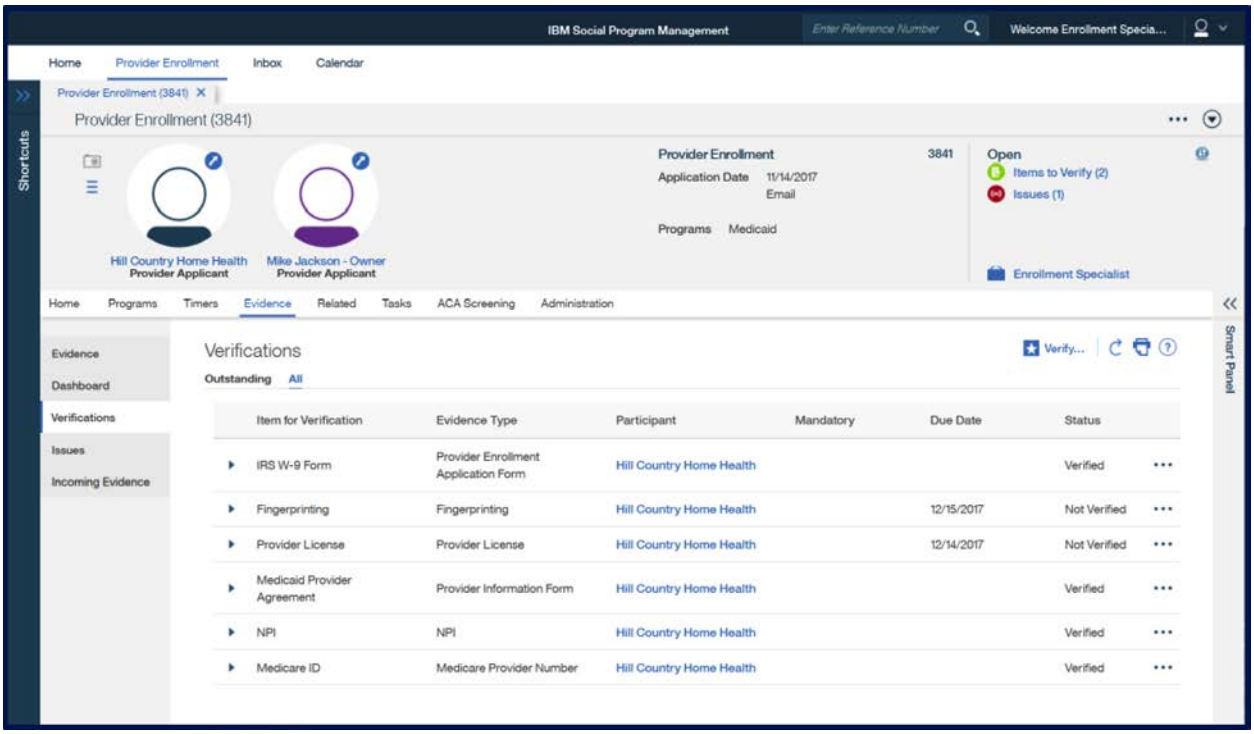


Figure 16: Application Verifications

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

Application ACA Screening:

The Provider Application Process requires screening to determine risk levels, the need for onsite visits, etc. The Application ACA Screening, as discussed in Requirement 5.5.14, displays the screening results.

Figure 17: Application ACA Screening

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

Provider Site Visit

The Risk Assessment performed as part of the Provider's application process determines the need for a site visit or evaluation. PMS will track and maintain details of site visits, all of which will be displayed on the Provider Site Visit screen. This is discussed in Requirement 5.5.17.

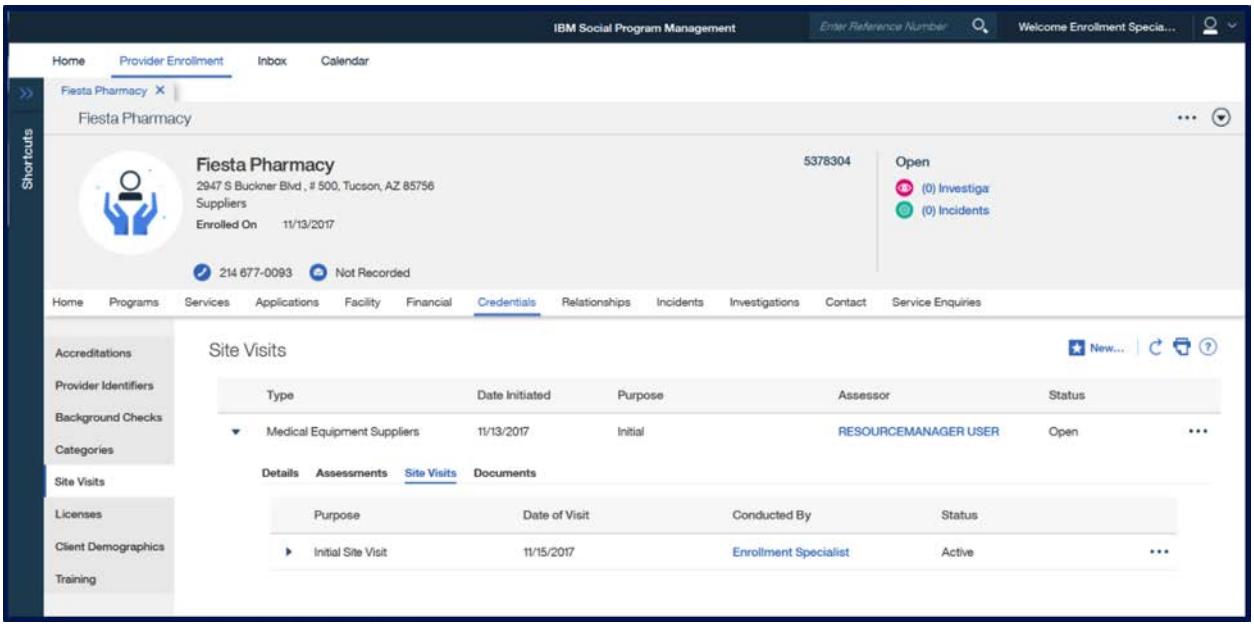


Figure 18: Provider Site Visits

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

Provider Notification

The PMS will track provider validation and revalidation periods and will produce notifications to the provider informing them of the need to revalidate their eligibility. The system can be configured to generate notifications at predetermined milestones, on a predetermined schedule, or as a result of an action or case event. The screen shot below provides a sample notification informing the provider that they must complete their revalidation process. This is further discussed in Requirement 5.6.3.

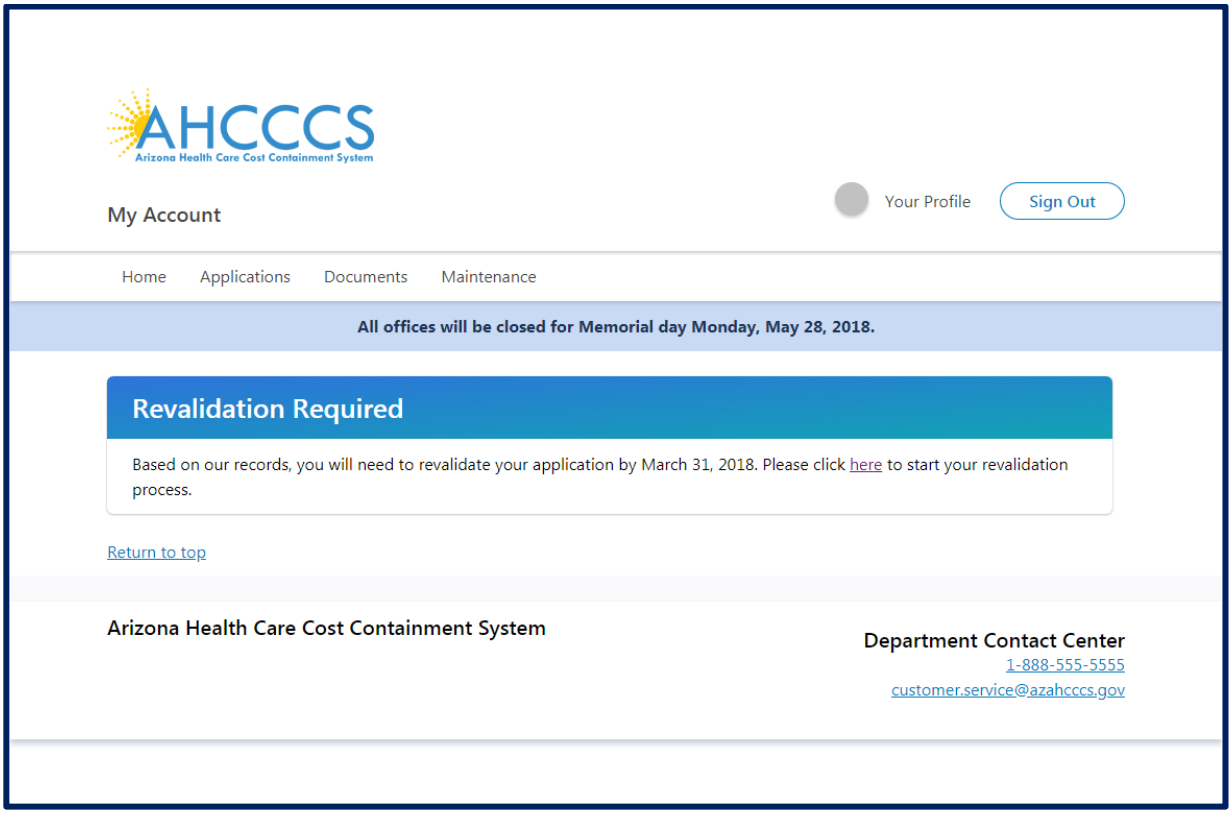


Figure 19: Provider Notification

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

Provider Types

A complete history, including effective dates, for each service type is maintained on the provider's record, as shown below. This is further discussed in Requirement 5.9.2.

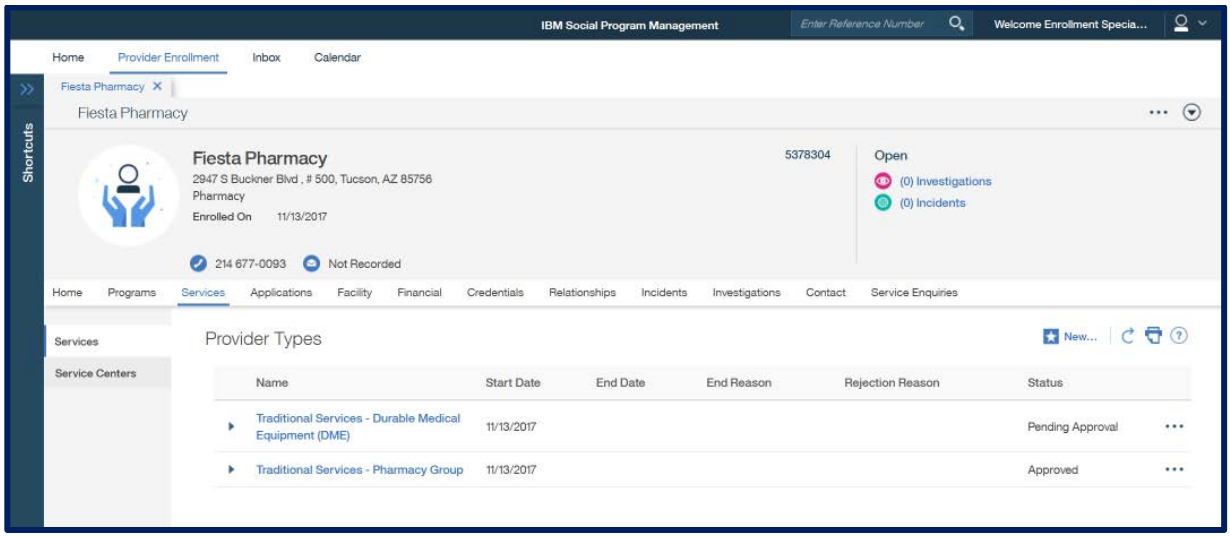


Figure 20: Provider Types

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

Application Home Page

The PMS maintains a transaction log, including auto-generated comments of any actions executed by the system. The Application Home Page, as discussed in Requirement 5.9.9, provides details of these transactions.

The PMS maintains a transaction log, including auto-generated comments of any actions executed by the system. The Application Home Page, as discussed in Requirement 5.9.9, provides details of these transactions.

The PMS maintains a transaction log, including auto-generated comments of any actions executed by the system. The Application Home Page, as discussed in Requirement 5.9.9, provides details of these transactions.

The PMS maintains a transaction log, including auto-generated comments of any actions executed by the system. The Application Home Page, as discussed in Requirement 5.9.9, provides details of these transactions.

The PMS maintains a transaction log, including auto-generated comments of any actions executed by the system. The Application Home Page, as discussed in Requirement 5.9.9, provides details of these transactions.

The PMS maintains a transaction log, including auto-generated comments of any actions executed by the system. The Application Home Page, as discussed in Requirement 5.9.9, provides details of these transactions.

The PMS maintains a transaction log, including auto-generated comments of any actions executed by the system. The Application Home Page, as discussed in Requirement 5.9.9, provides details of these transactions.

The PMS maintains a transaction log, including auto-generated comments of any actions executed by the system. The Application Home Page, as discussed in Requirement 5.9.9, provides details of these transactions.

The PMS maintains a transaction log, including auto-generated comments of any actions executed by the system. The Application Home Page, as discussed in Requirement 5.9.9, provides details of these transactions.

The PMS maintains a transaction log, including auto-generated comments of any actions executed by the system. The Application Home Page, as discussed in Requirement 5.9.9, provides details of these transactions.

The PMS maintains a transaction log, including auto-generated comments of any actions executed by the system. The Application Home Page, as discussed in Requirement 5.9.9, provides details of these transactions.

The PMS maintains a transaction log, including auto-generated comments of any actions executed by the system. The Application Home Page, as discussed in Requirement 5.9.9, provides details of these transactions.

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

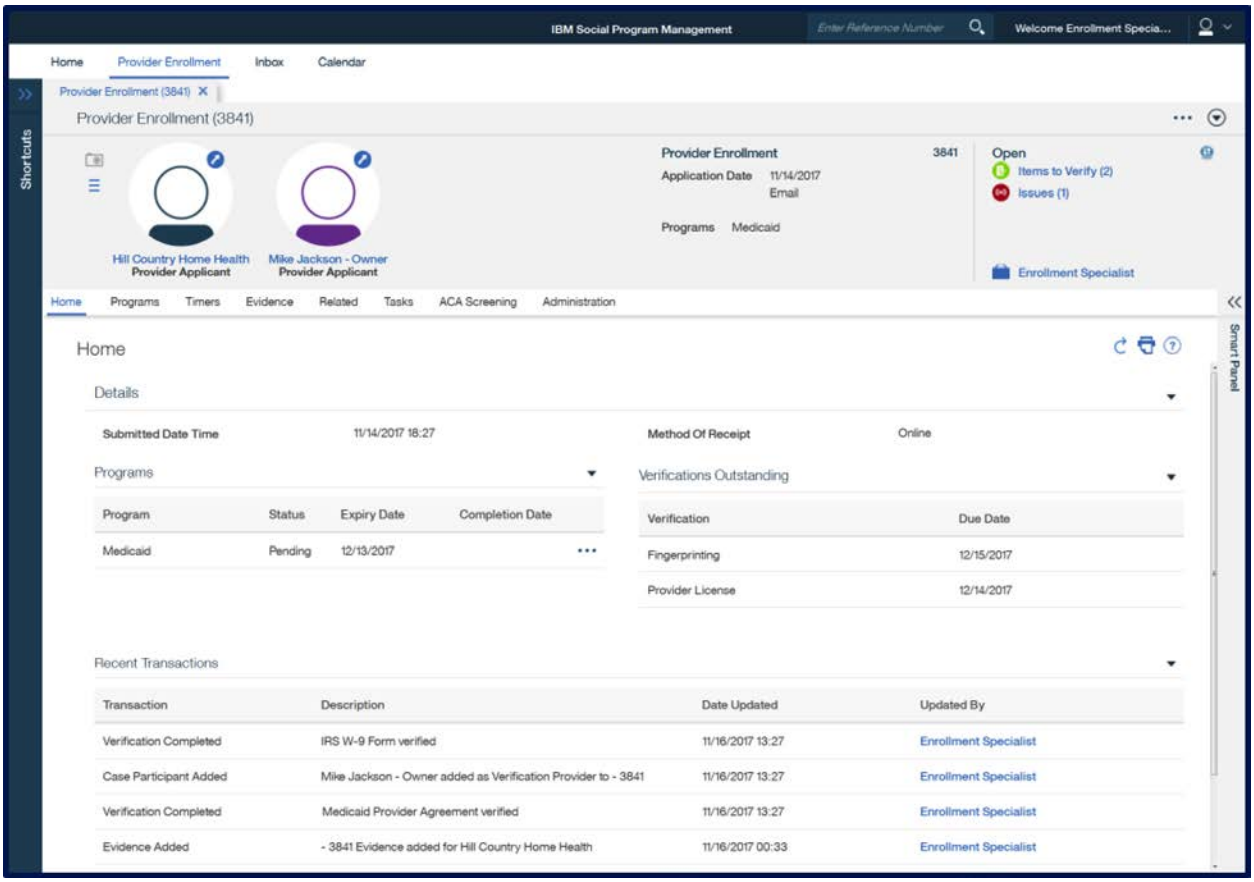
The PMS maintains a transaction log, including auto-generated comments of any actions executed by the system. The Application Home Page, as discussed in Requirement 5.9.9, provides details of these transactions.

The PMS maintains a transaction log, including auto-generated comments of any actions executed by the system. The Application Home Page, as discussed in Requirement 5.9.9, provides details of these transactions.

The PMS maintains a transaction log, including auto-generated comments of any actions executed by the system. The Application Home Page, as discussed in Requirement 5.9.9, provides details of these transactions.

The PMS maintains a transaction log, including auto-generated comments of any actions executed by the system. The Application Home Page, as discussed in Requirement 5.9.9, provides details of these transactions.

The PMS maintains a transaction log, including auto-generated comments of any actions executed by the system. The Application Home Page, as discussed in Requirement 5.9.9, provides details of these transactions.



Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

Figure 21: Application Home Page

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

APPENDIX B: PROJECT MANAGEMENT PLAN

This page intentionally left blank.

Stdihe sdheithd
Shetiehd
shiethd
thedivhee
shitshe
dhetieid
shdis'dcneaithe
ehiehsfhti
sh sithed
sheitehd
dheiedi
sheididv
djhritoahreohsmd hidrhiridhidhisrhdk h vjhdhfeiidhvh slahri dihdrhfibhrifi hdirhf

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

AHCCCS Provider Management System

[contract number]

Project Management Plan

VERSION 0.6

March 15, 2018

TABLE OF CONTENTS

1. Introduction 1
1.1.1 Purpose of the Project Management Plan 1
1.1.2 Project Characterization 1
2. Executive Summary of Project Charter 1
3. Overview 1
4. Assumptions/Constraints/Risks 2
4.1.1 Assumptions 2
4.1.2 Constraints 3
4.1.3 Risks 3
5. Project Scope 4
5.1.1 Requirements Management 4
5.1.2 Scope Statement 5
5.1.3 Scope Management 5
5.1.4 Project Work Plan (PWP) 5
5.1.5 Deployment Plan 5
5.1.6 Change Control Management 11
6. Overall Project Management Approach 11
6.1.1 Estimating 12
6.1.2 Schedule Management 13
6.1.3 Financial Management (Cost/Budget Management) 13
6.1.4 Earned Value Management 14
6.1.5 The Performance Measurement 14
6.1.6 Non-EVM Metrics 14
6.1.7 Quality Management 15
6.1.8 Staff Management 15
6.1.9 Communication Management 17
6.1.10 Risk Management 17
6.1.11 Configuration Management 20
6.1.12 Issue Management 20
6.1.13 Records Management 21
6.1.14 Acquisition Strategy 21
6.1.15 Software Process Improvement (SPI) 22
6.1.16 Security 22
6.1.17 Privacy 23
6.1.18 Business Continuity 23
6.1.19 Compliance Related Training 23
Appendix I: Record of Changes 25
Appendix II: PMP Acronyms List 25

Appendix III: Glossary 26
Appendix IV: Referenced Documents 27
Appendix V: PMP Approvals 28
Appendix VI: Additional Appendices 29

1. INTRODUCTION

This Project Management Plan (PMP) provides detailed plans, processes, and procedures for managing and controlling the lifecycle activities of the AHCCCS/Med-QUEST project. It describes the processes and approaches for managing (i.e., planning, executing, monitoring, and controlling) the project. The information in this PMP, and its subsidiary plans, provides the basis for communication and understanding among project team members and all other stakeholders.

1.1.1 PURPOSE OF THE PROJECT MANAGEMENT PLAN

The PMP documents the structure, processes, and resources that will be used to execute a successful project and create deliverables that meet the AHCCCS/Med-QUEST Provider Management System (PMS) contract requirements. This PMP covers the project organization, approach and timeline, work planning and controls, resource management, tools, and communication plans.

The PMP is approved by the sponsor and project leadership during project planning and is maintained throughout the life of the project. It is a living document that is kept up-to-date and should be considered the primary source for information about the PMS organization, stakeholder engagement in project activities, and project management processes, tools, and terminology. The PMS management team will review the PMP on a regular basis to confirm it is current.

The intended audience of the PMS PMP is all project stakeholders, including the project sponsor, senior leadership, and the project team.

1.1.2 PROJECT CHARACTERIZATION

Strategic Goals	• Streamline and reduce the burden of the enrollment process for providers • Ensure compliance with Medicaid requirements for program participation • Begin the process of updating a 30-year-old Pre-Paid Medicaid Management Information System (MMIS) shared by AHCCCS/Med-QUEST through modular system development and integration • Share provider enrollment data with managed care credentialing entities
High-Level Requirement	This system shall consolidate multiple provider enrollment applications currently in use into a single enrollment process that electronically collects and processes the information needed to support provider screening, enrollment, verification, and registration.

2. EXECUTIVE SUMMARY OF PROJECT CHARTER

See Project Objectives in Section 1 above.

3. OVERVIEW

The Arizona Health Care Cost Containment System (AHCCCS) is the single state agency for the State of Arizona. In that capacity it is responsible for operating the Title XIX and Title XXI programs through the state's 1115 Research and

Demonstration Waiver, which was granted by the Centers for Medicare and Medicaid Services (CMS), U.S. Department of Health and Human Services. As of June 1, 2017, AHCCCS provides coverage to approximately 1.9 million members in Arizona.

AHCCCS has over 70,000 active providers in Arizona, such as individual medical and behavioral health practitioners, therapy disciplines, institutions, durable medical equipment companies, and transportation entities.

Through an Intergovernmental Agreement, AHCCCS supports processing for the Hawaii Medicaid program (Med-QUEST), which provides coverage to approximately 360,000 members. Med-QUEST has approximately 8,100 active providers in Hawaii, such as individual medical and behavioral health practitioners, therapy disciplines, institutions, durable medical equipment companies, and transportation entities.

AHCCCS is leading a joint undertaking with Med-QUEST to streamline and reduce the burden of the enrollment process for providers. Streamlining the enrollment process will ensure compliance with Medicaid requirements for program participation and begin the process of updating a 30-year-old pre-paid MMIS shared by AHCCCS/Med-QUEST through modular system development and integration.

This system shall consolidate multiple provider enrollment applications currently in use into a single enrollment process that electronically collects and processes the information needed to support provider screening, enrollment, verification, and registration. In addition, AHCCCS/Med-QUEST is interested in a system with a credentialing capability.

The intent of consolidating and streamlining the provider enrollment process is to reduce the processing time and duplication of work by AHCCCS, Med-QUEST, and providers by allowing providers to submit data using one centralized interface, whether the provider is enrolling or revalidating, for all agency-supported programs. In addition, because much of the same information is collected both by AHCCCS or Med-QUEST (for registering and enrolling providers) and its contracted managed care entities (for provider credentialing), AHCCCS envisions that the system shall have the capacity to share provider enrollment data with managed care credentialing entities.

4. ASSUMPTIONS/CONSTRAINTS/RISKS

4.1.1 ASSUMPTIONS

Because a successful Agile implementation requires active stakeholder involvement during sprints and epic reviews, we assume the following primary contact points and subject matter experts will be available to our implementation team:

a. Identification and introduction to primary AHCCCS and Med-QUEST state PMS contacts within 2 days of contract start. This person will be responsible for management and delivery of the PMS application from the state's perspective; this individual is empowered to make decisions on behalf of the program or can quickly obtain a decision (within 48 hours).

b. Provider Enrollment Primary Contact Points for Enrollment, Online Provider Directory, Interfaces, Reporting, and Data Conversion must be identified within 3 days of contract start; these contact points are empowered to make decisions on behalf of the program or can obtain a decision (within 48 hours). These individuals will be responsible in their functional areas for ensuring, identifying, and coordinating the participation of state resources during initial discovery, JAD sessions, or requirement sessions. In support of the Agile framework, resources will be available to participate in managing product and sprint backlogs, review sprint deliverables, and be empowered to "accept sprint deliverables as done."

c. Provider Enrollment SMEs that can represent an end-to-end provider enrollment business process within 2 weeks of contract start. SMEs are individuals who have knowledge of current (legacy) systems, experience from technical and functional perspectives, and availability to work with Team NewWave.

d. Online provider directory SME who can represent requirements of the online provider integration process (business rules, data, frequency) within 3 weeks of contract start.

e. Data conversion SMEs identified within 3 weeks of contract start who have knowledge of current (legacy) systems where current provider data reside. State SMEs must have current system experience from a technical and functional

perspective and have the ability to work with Team NewWave in mapping current system data to the new PMS. Documentation requirements will include data dictionary (including business rules), logical and physical data models, and documentation related to accessing development and test systems for data analysis and testing.

f. Reporting SMEs identified within 3 weeks of contract start. SME available from each business area to represent unique requirements of their division.

g. Access to current reports and any user documentation describing report function, frequency, business rules, user access, or other pertinent data.

h. Integration SMEs identified within 2 weeks of contract start for each integration point (both internal and external). SMEs must have experience with integration requirements and work with Team NewWave to define data requirements, frequency, and other requirements that must be considered. Access to current integration documentation (if available), including interface description, layout, frequency, or other relevant data.

i. Availability of vendor to support discussions related to integration with MMIS and process requirements.

4.1.2 CONSTRAINTS

No constraints have been identified relative to this PMP at this time.

4.1.3 RISKS

Implementation/Transition

1. Accurate and complete capture of all requirements for use cases
    a. Mitigation: Quickly onboard experienced Business Analysts (BAs) with Cúram and Cognos
2. Availability of business owners to support requirements development and capability acceptance
    a. Mitigation: Ensure AHCCCS and Med-QUEST primary contacts and SMEs are identified, informed, and committed
3. Availability of qualified contractor staff to meet milestones
    a. Mitigation: Identify SMEs, coordinate transition and transfer timelines, and provide clear subcontract staffing plans
4. Availability and capacity of infrastructure services
    a. Mitigation: Early negotiation of Joint Operating Agreement to define roles and responsibilities and SLAs

Internal & External System Interfaces

5. Accurate and complete capture of all requirements, by milestone schedule
    a. Mitigation: Quickly onboard experienced BAs
6. Access to external resources and data to meet milestones
    a. Mitigation: Coordinate Joint Operating Agreements before contract start

Data Conversion/Migration/Consolidation

7. Access to all internal and external database schemas and data definitions and descriptions for Data Conversion Plan
    a. Mitigation: Coordinate Joint Operating Agreements before contract start
8. Timely approval from business owners of data mapping plan
    a. Mitigation: Schedule early coordination and sufficient time for review cycle

5. PROJECT SCOPE

5.1.1 REQUIREMENTS MANAGEMENT

5.1.1.1 Implementing COTS Solutions using Agile Methods

When organizations acquire a COTS solution, but then try to undertake extensive customization of the application to fit their existing business practices, rather than use the functionality that is available out of the box, it can add unnecessary time and complexity to the implementation.

Following Team NewWave's Agile Development Methodology can avoid this common problem because our methodology focuses on the outcomes the business is trying to achieve and then identifies how best to use existing capabilities within the COTS product to achieve these outcomes, rather than focusing on detailed low-level requirements that are generally based on the current practices.

Our methodology enables customers to achieve maximum value from the functionality they have acquired in the COTS product and reduces the time and effort needed to specify basic functionality that is available out of the box, freeing up the project to focus on the important areas of the solution that provide the most business benefit.

Team NewWave's delivery approach starts with the Product Discovery Phase.

5.1.1.2 Product Discovery Phase

During the Product Discovery phase, Team NewWave captures what outcomes AHCCCS/Med-QUEST is trying to achieve and conducts workshops as needed to finalize the business solution. The business solution is delivered during the Product Delivery phase using an Agile development approach. The approach identifies what outcomes are essential at the very start of the project. For example, identifying the business needs, the business processes the solution is required to support, and any business priorities for the solution, and then flows these artifacts through the lifecycle of the project.

This business solution initially identifies the outcomes that the business is trying to achieve; these are defined in Features and then grouped into Epics, which define a large area or body of work. The Epics are useful for planning key points within the project. Delivering all the functionality within an Epic means that a large piece of business value has been provided. Epics are also useful for holding usability sessions (Business Playback) with a wider audience. Being able to demonstrate what has been delivered, but in the context of a business feature, means that the users within the organization can picture how the functionality will work within their organization. Features can also be linked to the functional areas within Cúram to allow for a more focused development approach.

Agile aims to deliver value at the end of each sprint, so Epics and Features are broken down into User Stories that are used to estimate and manage the development and that can also be used to create Tasks that are assigned to individuals to develop. A Task can be for anything—it could be for code, production of a supporting document, or other task.

User Stories are used in Scrum to document requirements, to identify the scope of sprint planning, and for estimating purposes. User Stories are short descriptions of a feature told from the perspective of the person who desires the new capability, usually a user of the system. User Stories are developed to be understandable to business users and technical developers. They typically follow a template as follows:

As a <type of user>, I want <some goal> so that <some result/benefit>.

User Stories are typically derived during or just before sprint execution and should always align with the sprint goals to ensure the ultimate development of that User Story is aligned with that sprint's objectives. During sprint planning, User Stories are further developed.

When building anything, whether a house, software, or a business, it is necessary to have a solid baseline to build on—this is also true for agile development. Our approach ensures that the technical foundations of the project are well understood, including the performance required for the application, the systems it must interact with, and any legislation or security requirements an organization may have. These elements can affect the way a solution is architected and must be understood at the start of the development of the project. We will use the technical requirements from the SOW to help design the high-level technical solution

that meets the organization's needs. These can still be defined as User Stories and developed via the normal story and scrum approach.

The key product produced is the Product Backlog that has completed its prioritization process.

5.1.2 SCOPE STATEMENT

Team NewWave will provide services for managing, implementing, operating, and supporting the Provider Management System for AHCCCS and Med-QUEST. This support is wide-ranging, covering areas such as the following:

- Implement and configure a COTS Provider Management System
- Ensure compliance with CMS requirements for obtaining a CMS certification
- Support provider screening, enrollment, and verification processes
- Provide SMEs, training, and materials to AHCCCS and Med-QUEST trainers
- Provide a responsive and mature project management capability
- Provision and manage a secure, cloud-based data center
- Provide network, server, and storage management
- Establish configuration management and change control
- Ensure IT security policies and procedures are implemented and followed
- Perform system, integration, performance, and regression testing
- Support AHCCCS and Med-QUEST User Acceptance Testing (UAT)
- Ensure reliable Tier 2 and Tier 3 issue resolution and escalation
- Provide disaster recovery provisioning and operations
- Establish a continuous improvement across the Provider Management System.

5.1.3 SCOPE MANAGEMENT

Scope management is the responsibility of the PMS Project Manager. The PMS scope is defined by the contract SOW and AHCCCS-approved PMP, Project Work Plan (PWP), and funding. All work performed is defined in the PWS PWP and documented and tracked in the PMS schedule. If a question arises as to whether specific tasks are beyond the scope of the SOW, the PMS Project Manager addresses the issue with the AHCCCS contracting officer (CO) and their representative (COR).

The scope of the PMS project is detailed in the SOW and in the associated Team NewWave response (in the form of the technical proposal submitted March 15, 2018). Any new or proposed changes to this predefined scope inventory will be ratified through mutual assessment, clarification, and elaboration with AHCCCS. This will ensure the definition and content of each scope item is clear and acceptable to AHCCCS and all stakeholders. Any changes to a scope item are subject to review and sign-off by AHCCCS. The project team will focus only on those tasks and related items that directly support the approved project scope items.

Scope changes are anticipated in a program of this complexity and importance. Our scope management process follows our Requirements Management Process and tracks how and by whom a change is initiated, assessed, and integrated into the program documentation and project plan (when approved). Changes to cost and schedule are documented and communicated to AHCCCS so that a fully informed decision may be made regarding the scope change. We will not proceed with any work that may be considered outside the scope of this contract without written consent from AHCCCS.

5.1.4 PROJECT WORK PLAN (PWP)

Refer to Appendix D for the detailed Project Work Plan Task List and Deliverables.

5.1.5 DEPLOYMENT PLAN

Team NewWave's delivery approach continues with the Product Delivery Phase.

Approach:

Team NewWave tailored our proven Agile Development Methodology (ADM) to include IBM's Agile Cúram Delivery Approach to provide the best opportunity for completing the implementation of IBM's COTS product, Cúram, within the 9-month window required by AHCCCS.

Our ADM encourages a flexible and decentralized approach to software delivery in which team members respond to changing environments through continuous feedback and collaboration. Transparency along with continuous feedback and continuous integration and automation is key to quality software implementation.

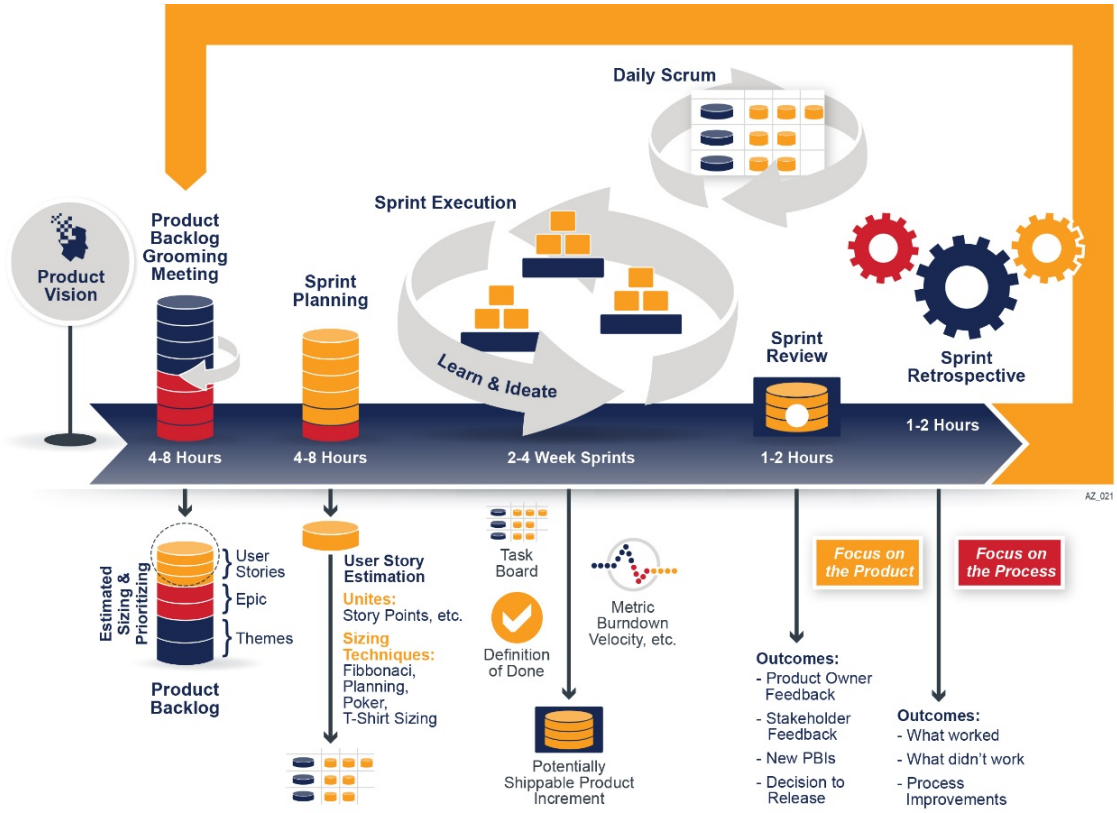
Our ADM incorporates the following best practices:

- Developing the application iteratively to ensure small, continuous improvement
- Implementing a short feedback cycle that allows users to provide feedback earlier in the process
- Continually managing requirements and adapting to change, replacing cumbersome change request processes
- Continually verifying quality
- Establishing a clear definition of "Done."

Structure:

Projects for mission-critical systems are inherently difficult and complex. The best way to approach them, therefore, is the same way we approach big projects in life: break them into smaller pieces. We construct the delivery as a series of iterations (sprints).

Each sprint implements capabilities to satisfy defined User Stories. A series of sprints implement Features and Epic functionality of our solution. There are multiple processes for performing a sprint; Team NewWave's ADM uses the most common process, the Scrum. The figure below provides a view of the Scrum process for performing a sprint.



On completion of each sprint, the product owner (AHCCCS/Med-QUEST) approves demonstrated product capabilities of our solution and prioritizes and grooms the product backlog. A series of sprints is used to implement the Features and Epic functionality of our solution. On completion of each Epic, we conduct a business review or playback to a wider audience of stakeholders. The figure below provides a high-level overview of this process.

Roles & Responsibilities:

There are four roles within the Scrum methodology: Product Owner, Scrum Master, Development Team, and Stakeholders. A critical success factor for Scrum is collaboration and communication across the roles. The table below describes in detail each role and the accountabilities of each.

Rules of the Road:

1. No one person can serve multiple roles. (i.e., a Scrum Master cannot also play the role of Product Owner).
2. The Scrum Master is preferably not the Project Manager.
3. The Scrum roles allow for a balance of power across the roles so no one role has unfair authority over the other roles.

Role	Role Description
Product Owner	• Voice of the customer • Responsible for Product Vision • Prioritizes backlog • Articulates business requirements or can bring together appropriate resources to ensure accurate communication of requirements • Accepts or rejects each product increment (Sprint)
Scrum Master	• Champion of the Scrum team and facilitates the Scrum process • Facilitates Sprint Planning, Daily Scrums, Sprint Reviews and Sprint Retrospectives. • Maintains the focus of the team. • Serves as a coach and mentor to the Team. • Assists in resolving impediments identified within sprints • Works with Team and business to implement improvements
Development Team	• Champion of the Scrum team and facilitates the Scrum process • Facilitates Sprint Planning, Daily Scrums, Sprint Reviews, and Sprint Retrospectives • Maintains the focus of the team • Serves as a coach and mentor to the team • Assists in resolving impediments identified within Sprints • Works with the team and business to implement improvements
Stakeholder	• Cross-functional team (e.g., business analysts, developers, solution architects, testers, DBA, security, operations) of individuals that is accountable for delivery of tasks within the Sprint • Works with the Product Owner to analyze and decompose the Product Backlog • Performs User Story estimation for each Sprint

Role	Role Description
	• Attends all Scrum meetings • Collaborates and shares knowledge and experience with the team, Product Owner, and Stakeholders • Assists other members of the team • Negotiates commitment with the Product Owner; one sprint at a time • Self-organizing • Functions best when co-located
	• Other individuals within the organization that may be end users of the product or are interested in ensuring product delivery is successful

Three Artifacts:

The following Scrum artifacts are produced via the Jira tool, which is the agile tool used by Team NewWave.

Artifact	Artifact Description
Product Backlog	• An ordered list of prioritized requirements that is maintained for a product. It consists of features, bug fixes, non-functional requirements, and other items; includes what must be done to successfully deliver a viable product. It consists of the: o Why (requirement) o What (user stories) o How (technical tasks; determined by the Development Team) o Aspects of a "Healthy" Product Backlog: Features, Estimated, Prioritized • The product backlog is a living list of features, bug fixes, non-functional requirements, and other items that can be re-prioritized by the Product Owner.
Sprint Backlog	• Sprint backlog includes items from the Product Backlog that have been agreed on for delivery within the current sprint. • Contains stories that will not change during the sprint, allowing the team to focus on delivering the selected stories. • Outside the Sprint Backlog, the Product Owner can re-prioritize stories if needed. • A good Sprint Backlog contains 6–10 stories. • A Sprint should last no longer than 20 business days. • Multiple sprints can be planned to support a release.
Burndown Chart	• A graphical representation of work left to do versus time left to do it. • The outstanding work (or backlog) is often on the vertical axis, with time along the horizontal. • That is, it is a run chart of outstanding work. It is useful for predicting when all of the work will be completed.

Execution:

Our preferred approach for delivering capabilities is to use the Scrum Framework, which focuses on delivering value by providing the customer with "shippable components" of capability through time-boxed and iterative increments (i.e., sprints). Scrum is a disciplined agile development process that allows teams to deliver usable product increments in an iterative process, absorbing change and new requirements as the project proceeds. A Product Backlog provides for the prioritization of Features, User Stories, or Tasks that are required to deliver the end product to the customer. The backlog is used to further decompose the work into smaller work efforts (known as sprints), with each sprint being validated by the customer. The result is a potentially shippable product (production ready).

After the Backlog Prioritization process is completed, sprint planning is initiated. This meeting should take no more than 4–8 hours and be based on the delivery of prioritized items by the Product Owner. In planning for the first sprint, the team estimates how many story points that it can complete in a 2- to 4-week period. This duration includes development, testing, sprint review, and sprint demonstration.

On completion of the first sprint, adjustments are made for Sprint 2 based on Sprint 1 results and input from the team.

Within the Scrum process there are five Scrum meetings or ceremonies, each serving a unique objective in supporting a customer-focused and iterative process to meet the Product objectives.

Ceremony	Ceremony Description	Output(s)
Backlog Refinement Meeting	• Prioritization of Backlog by Product Owner • Estimates provided on Product Backlog Items (PBI)	Product Backlog Tool: JIRA
Release Planning	• Planning of multiple sprints to predict when a release might be delivered • Split big Product Backlog Items (PBI); also called Epics into User Stories • Analyze PBI • Estimate and re-estimate PBI • Prioritize and re-prioritize PBI for future Sprints *Frequency*: Once at beginning of each Release.	Release Plan Tool: JIRA
Sprint Planning	• Determine scope and timing of upcoming Sprints Typically divided into two parts: • *Part 1—What:* - At beginning of each Sprint the Product Owner and team review the high-priority items in the Product Backlog that the Product Owner is interested in implementing - Team understands what the Product Owner wants and why it is needed - Product Owner and team negotiate which PBI will be converted to working product during the Sprint - Define the Sprint Goal: Summary Statement of the Sprint Objective • Part 2—How: - Team forecasts the number of items it can complete by the end of the Sprint, starting with the highest priority - Sprint Commitment: Team sets a realistic target for what it believes it can deliver by the end of the Sprint • Sprint Estimation—hours or story points • A sprint should run 2 to 3 weeks to complete	Sprint Backlog Tool: JIRA

Ceremony	Ceremony Description	Output(s)
	• Multiple sprints can be planned to support a release • No changes are accepted until the next sprint (a general rule; understanding that exceptions may arise) *Frequency*: Beginning of each Sprint	
Daily Scrum	• Short 15-minute standing meeting that occurs every workday • All team members attend and report on the following: - What they have accomplished since the last meeting - What they will do before the next meeting - What obstacles are in the way • Monitoring and controlling of Sprint accomplished via a Sprint Burndown Chart • Tasks can be re-estimated daily if required as new information is obtained • If sprint tasks cannot be completed within the defined sprint, then tasks should be moved to a future sprint • Scrum Master helps team resolve and remove roadblocks • Only members of the team who are performing the work participate in the Daily Scrum, although others may observe *Frequency*: Once per day	Updated Sprint Task List Updated Sprint Burndown Chart Impediments List Tool: JIRA
Sprint Review	• Review of functionality developed during a Sprint • This is the "inspect" part of the inspect and adapt process; performed at the end of each Sprint • Time for team to celebrate its accomplishments, demonstrate work finished within the iteration • Receive immediate feedback from project stakeholders • Real users and Product Owner have hands-on interaction with the software, rather than passive-session demonstration from the team *Frequency*: At the end of Sprint or Milestone	Release Burndown Chart Tool: JIRA
Sprint Retrospective	• Review processes and identify opportunities for improvement • This is the "adapt" part of the inspect and adapt process; performed after the Sprint Review • Team discusses what is working and not working and agree on changes • Ensure a focus on positives and strengths, not only on problems *Frequency*: At end of a sprint	Agreed Actionable Improvements Tool: Confluence

On completion of each Epic, we conduct a business playback session to a wider audience, which normally takes the form of an all-day workshop where a walkthrough is presented on the business functions that have been developed, and a demonstration of

the functionality is provided. These playback sessions demonstrate progress to key stakeholders and sponsors on how the application is viewed by end users of the application.

The business playback should also include the organization's UAT testers. If these testers attend the playback sessions means they are able to see first-hand whether or not the functionality provided meets the business need. Thus, when they are scripting and testing, they do not need to try to work out whether or not the functionality is as per the business need, but instead just need to test that what was agreed on works within the organization's test environment. This saves time and effort for everyone because the testers reduce the effort needed to document tests and the time they spend raising issues. The Scrum team saves a large amount of time reviewing what has been raised by the testers and the time required in responding to these issues.

5.1.6 Change Control Management

A strong change management program is necessary to establish processes and procedures for managing change and the associated risks and for ensuring adherence to such processes. Team NewWave provides change management services consistent with ITIL, CMMI, and the CMS XLC, which includes adherence to change management processes and implementation, customization, administration, enhancement, and use of processes and tools. Change management for the Provider Management System is handled in accordance with the Change Management Plan, a subsidiary plan to this PMP. We will tailor our Change Management Plan to meet the needs of AHCCCS and Med-QUEST.

For all changes to the PMS environments, we perform an internal review of change plans and their potential impacts. Once a change is approved by our quality assurance and services manager and the affected operational managers, we document the proposed changes; the rationale for and impact of the change; and the implementation, testing, and back-out plans. We will present the proposed changes to the AHCCCS/Med-QUEST Configuration Control Board (CCB) for approval and include approved changes in the weekly change coordination meeting and in the calendar of planned changes. On approval, we will include the configuration changes in Jira. We will enhance the change control process by automating the approval process for low-risk changes, allowing the weekly CCB meeting to focus on medium- to high-risk changes in the PMS environment. All approved changes to the Provider Management System or its environments will be reflected in updated in the appropriate documentation within 10 days of taking affect.

The PMP will undergo an annual review for incorporating changes. The updated PMP will be coordinated with AHCCCS for approval and the signatures in Appendix E.

6. Overall Project Management Approach

All NewWave projects follow our standard project management, development and/or services practices, which are housed in our NewWave Process Asset Library (PAL) on our internal SharePoint site. All projects follow our standard NewWave Project Management Methodology, but each project can tailor its assets to meet the specific needs of the customer and the SOW requirements.

Team NewWave's disciplined management approach integrates program, project, and technical management at all levels, and includes the following important components for successful project management:

- Initiate and Plan: Comprehensive project initiation and planning are the cornerstones of our projects. This includes a PWP, Project Management Plan, and associated control plans.
- Execute: Plans are followed, work is performed; plans are adjusted as necessary; Agile management practices are applied as much as possible.
- Monitor, Measure, and Report: Performance is monitored, metrics are collected and analyzed, and reports are generated (including metrics, lessons learned, peer reviews, other reports, and dashboards).
- Quality Management: Quality is reviewed, reported on, and monitored throughout the life of the program.
- Communicate and Collaborate: Comprehensive and consistent communication with AHCCCS and other stakeholders throughout the program is essential for PMS to be successful.
- Continuous Improvement: Communication, feedback, and lessons learned from all stakeholders ensure processes and work products continue to improve.
- Governance: NewWave's corporate Project Management Office (PMO) provides support and guidance.

During the initiation and planning phases, Team NewWave assesses and applies our standard project management, development, and services practices and tailors all of project documentation and processes from our standard NewWave Project Management Methodology to comply with our contract and AHCCCS/Med-QUEST requirements.

NewWave provides project management and will develop and update project management artifacts as required by AHCCCS/Med-QUEST and the NewWave PMO. This contract includes providing all personnel and other resources, except as otherwise specified by AHCCCS, necessary to accomplish the work defined in the contract SOW.

Our NewWave PMO and quality assurance teams will conduct periodic QA reviews of activities and work products to monitor our adherence to processes and procedures. The PMS project measurement and analysis process will support tracking of actual performance against established plans and objectives. Our processes are designed with continual process improvement as a goal.

The goals of our PMS project management processes are to balance the available budget, resources, and functionality while providing quality service that meets SOW requirements and satisfies AHCCCS. Periodic meetings are held to assess the health of the project (i.e., to review and monitor progress, assess resource needs, maintain the project schedule, address outstanding issues, and manage and mitigate risk).

6.1.1 ESTIMATING

The Scrum methodology leverages an estimation technique referred to as story points. Story points are different from hourly estimates because the story points measure complexity and hours measure effort.

The foundation of story point estimating is that a single user story is identified and estimated as a relative measure. The team should identify a user story as a baseline and use that story point estimate as a guideline to estimate future user stories. This baseline can change as sprints and a better understanding of the product deliverable are identified and clarified by the Product Owner.

For the purposes of estimating, we recommend using either Tee Shirt sizes or the Fibonacci method. Tee shirt size estimating user story sizes are based on a Small (S), Medium (M), Large (L), or Extra Large (XL) complexity scale. Once the user story is assigned a tee shirt size, it must be translated into a number for use in Agile Jira.

Tee Shirt Size	Numerical Equivalency
S	1
M	3
L	5
XL	7

The Fibonacci method leverages a numerical complexity scale of 1, 2, 3, 5, 8, 13, and 21 to assign to each user story. The idea is to initially identify a user story that is of medium complexity and then use that user story for estimating go-forward user stories. Both estimating methods require the team to complete 2–3 sprints to begin to see a normalization of the estimating complexity and to become more accurate on how many user story points can be completed in a sprint. Story points are used to estimate user stories; hours are used to estimate at the task level that link to a user story.

Estimating Process:

1. Identify one or more items from the Backlog and perform a relative sizing of that item.
2. Walk through the requirements of that story.
3. Document any additional details identified during the discussion.
4. Questions to ask when sizing:
   What do we need to learn before we start the work?
   What is the development effort required?
   Automation of acceptance tests?
   External dependencies?
   Have we done a similar story that we can use as a starting point?
5. Team will reach a consensus of the size of the story per the definition of done.
6. As part of the retrospective, continue to assess the relevant story point to ensure it is still valid.

In gaining concurrence of the team as related to the user story size, an approach called Poker Planning can be used to prevent biases and give equal weight to all involved. Each team member has a set of cards that represent the sizing methodology being used and each team member plays a card that represents its estimate. If there are differences among team members' estimates of the proposed sizing, then discussions occur until the team agrees on the size. This should not be a lengthy process to reach an agreement on size. It is important to remember that retrospectives are held and adjustments are made based on the actual results.

6.1.2 SCHEDULE MANAGEMENT

Team NewWave has established a project schedule baseline as part of the Project Work Plan. We will monitor progress against the baseline weekly. The project manager is responsible for ensuring the project schedule is updated with the latest information and never more than 3 business days out of date.

The project coordinator maintains the project schedule throughout the project. The project schedule indicates the tasks to be executed, WBS number, duration, resources, planned start and end dates, percent complete, actual end dates, internal and external reviews, milestones, and dependencies.

Our approach begins with a definition of scope, identification of assumptions and constraints, definition of task activities, logical sequencing of events, and an estimation of the level of effort and task duration. This sets the foundation for monitoring and controlling project progress.

Team NewWave uses Microsoft Project as our scheduling tool. The Gantt chart, network diagram, resource usage, task usage, and other standard reports from MS Project illustrate the project status and external dependencies and their impact on the overall schedule. The schedule allows for easy identification of the critical path, project milestones, and key deliverables.

The members of the PMS management team send their schedule updates to the integrated master scheduler weekly, and the updates are applied to the master schedule. The current version of the schedule is submitted to AHCCCS monthly. Individual sprints are tracked in Jira/VSTS.

6.1.2.1 Milestones

Detailed milestones are established for key internal and external deliverables to allow for forward planning and effective management and measurement of status against the plan. Appendix D contains the Project Work Plan Task List and Milestones.

6.1.2.2 Project Schedule

See the Project Work Plan in Appendix D of the Technical Proposal.

6.1.3 FINANCIAL MANAGEMENT (COST/BUDGET MANAGEMENT)

The project manager has overall responsibility for verifying that project resources are being expended according to the principles outlined in the SOW. Provider Management System team members document their work time daily. NewWave uses Microsoft Dynamics-NAV as our accounting system, including time recording. The project manager, in conjunction with the NewWave Finance Department, has established categories and charge codes to which time is allocated. Charge codes, once approved, are entered into the timekeeping system so members can log their time daily. The NewWave Finance Department maintains access to the charge codes and, on request, adds members to the specific charge codes they need to log their time accurately.

The project manager tracks the project burn rate and forecasts estimate to complete (ETC) and estimate at completion (EAC) using a combination of output of our accounting system, JAMIS (actuals), and projected and planned workbooks with ETC and EAC formulas.

Invoices are generated monthly from NewWave's accounting system and submitted to:

<Name and contact information of the individual to whom invoices are sent>

6.1.4 EARNED VALUE MANAGEMENT

The Provider Management System project does not have an EVM requirement.

6.1.5 THE PERFORMANCE MEASUREMENT

NewWave maintains a corporate measurement repository (Performance Vault) for all project metrics. This enables us to share metrics across the organization, and we benefit from lessons learned and knowledge sharing. Our plan for performance measurement for the PMS project is described in the PMS Project Measurement and Analysis Plan, a subsidiary plan to this PMP.

6.1.5.1 Key Success Factors

Primary stakeholders will consider NewWave—

- Develops and executes the PMP and initial schedule
- Participates in a project kickoff meeting with AHCCCS/Med-QUEST that includes:
    - Technical approach overview
    - Introduction of key personnel
    - Key deliverables and tasks
- Develops a solid implementation strategy
- Effectively communicates with all project stakeholders
- Provides on-time submission of required deliverables
- Delivers monthly status reporting that is timely and accurate
- Provides monthly financial and variance reports that are timely and accurate
- Participates in and facilitates the execution of weekly meetings and conference calls.

6.1.6 NON-EVM METRICS

The plan for performance measurement for the PMS project is described in the PMS Project Measurement and Analysis Plan, a subsidiary plan to this PMP.

The table below shows a sample of the standard Agile metrics we use on all development and operations and maintenance (O&M) projects. Additional metrics will be identified and documented in the final PMP.

MEASURE	METRIC	OBJECTIVE
Velocity Ratio	(Current sprint velocity) – (Baselined velocity)/Baselined Velocity	Tracks velocity trend
Story Acceptance Ratio	No. of Stories accepted / No. of Stories in Sprint	Measures the quality of deliverables
Story Completion Ratio	No. of Stories accepted / No. of Stories planned in Sprint	Measures the budget and timeliness of deliverables
Productivity	Actual effort / No. of Story points	Measures team productivity

The Project Metrics Summary image below shows an example of NewWave metrics results over an 8-month period, including development metrics, such as burn rate, velocity, and defects, and service metrics, such as tickets closed and average time per ticket. The metrics depict a variety of stop light results.

Project Metrics Summary	January	February	March	April	May	June	July	August
1. Percent of on-time deliverables	100%	100%	100%	99%	99%	100%	100%	100%
2. Percent of milestones completed on-time	100%	100%	100%	100%	90%	100%	100%	100%
3. Percent of client-facing deliverables peer reviewed	100%	100%	83%	82%	83%	100%	100%	100%
4. Average CPAR score	3.6	3.5	3.5	3.5	3.5	3.5	3.5	3.5
5. Percent of sprints accepted by customer per release	100%	100%	100%	100%	100%	100%	100%	100%
6. Burn rate	95%	84.5%	51.5%	77%	79%	119.5%	115%	94.7%
7. Defect rate	7.65%	2.45%	1.17%	0.25%	0.5%	1.5%	0%	0%
8. Percent of code covered by unit testing	66%	86%	86%	86%	86%	86%	86%	86%
9. Velocity rate	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
10. Percentage of successful builds	100%	100%	100%	100%	90%	100%	100%	100%
11. Percentage of automated test coverage	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
12. Number of HD tickets received each month	413	434	210	157	152	209	114	147
13. Number of tickets closed each month	553	602	340	250	218	235	243	143
14. Total open active tickets per month	249	197	163	144	123	206	110	117
15. Average open time per ticket	22.71	31.01	40.02	21.59	20.61	16.04	30.18	70.75
16. Percent of tickets exceeding SLA	11%	18%	16%	5%	4%	1%	7%	0%

AZ_020

6.1.7 QUALITY MANAGEMENT

Our plan for quality management of the PMS project is described in the PMS Quality Management Plan, a subsidiary plan to this PMP.

6.1.8 STAFF MANAGEMENT

The PMS project team is shown in the Organization Chart in Appendix B. The team is managed by our Project Manager, Tim Breland. Key personnel roles and qualifications are listed in the table below.

Role	Description	Qualifications
Project Manager	Primary point of contact (POC) with the state for contract performance, project management and scheduling, correspondence between the state and contractor, and status reporting to the state.	Certified PMP with at least 8 years of experience in managing personnel and/or enrollment activities. Previous Medicaid or similar healthcare system experience required.
Implementation Manager	Serves as designated POC for all system implementation and transition activities. The Transition Project Manager shall not serve in any other key personnel position during transition.	Certified PMP with at least 4 years as a project manager and 2 years as a project manager for a similar provider enrollment system.
Functional Lead (Cúram)	Responsible for providing subject matter expertise in Cúram functional and system capabilities.	At least 2 years of experience in using Cúram for providing healthcare systems management.
Functional Lead (Enrollment	Responsible for assisting state staff with provider enrollment processing subject matter and system-	At least 2 years of healthcare systems management and provider enrollment and

Role	Description	Qualifications
Processing)	level expertise.	network management experience.
Functional Lead (Reporting/Data)	Responsible for assisting state staff with data analysis, ad hoc report generation and production, scheduling data file download requests, monitoring and analyzing production reports, and dashboard reporting.	At least 2 years of experience in a combination of ad hoc, database, and report writer software and middleware and web-based reporting.
Quality Assurance Manager	Responsible for overseeing all provider enrollment data quality and testing. The quality manager may not perform in any other position.	A minimum of 2 years of experience with provider enrollment and Medicaid program integrity activities. At least 1 year of experience in managing personnel.

We selected PMS project team members specifically to meet the SOW requirements. All team members report to the project manager. The management team will conduct periodic staffing reviews to identify new resource needs and available resources and will adjust resource assignments as necessary. If new work is defined by a SOW modification, the project manager and the management team will determine the skills necessary to successfully deliver in accordance with the SOW.

The PMS team will use internal staffing processes and resources if a replacement is necessary. As resource requirements are identified, the project manager will prepare a requisition that highlights the skills, experience, and educational background required for the candidate. A human resources consultant will work with the project manager to identify both internal and external candidates and will manage the interview and hiring process.

NewWave will provide AHCCCS/Med-QUEST with notification and justification when substitutions for key personnel are required. Replacements for key personnel will have qualifications equal to or exceeding the qualifications of the individual being replaced.

6.1.8.1 Project Team Training

Through NewWave's comprehensive training program, we sustain a training focus that ensures employees have the training they need to perform the essential functions of their roles within the Provider Management System project team, while also providing professional development opportunities. Every staff member receives new--hire training, which consists of internal corporate processes, compliance, security, and HIPAA training.

NewWave also maintains a Learning Management System (LMS), which provides a comprehensive project management, business and technical content library. Staff members access the LMS to take advantage of the many learning opportunities and to improve their knowledge and skills.

Project-level training needs are assessed annually, and individual training needs are established during the staff performance review process. We are agile in our ability to deliver training based on the needs of the project.

The Provider Management System Project Training Plan will be completed post award.

6.1.8.2 Roles and Responsibilities

The PMS project manager has ultimate responsibility for verifying that staff members are working under documented expectations, responsibilities, and roles that are aligned with the needs of the PMS project. The project manager will work with the project team to document, communicate, manage, and evaluate these expectations for each team member using a responsible, accountable, consulted, and informed (RACI) matrix. Project team members and stakeholders are evaluated annually based on the agreed set of expectations. Expectations and goals also are updated annually or when a change in assignment occurs. Roles and responsibilities for each project team member and stakeholder are defined in the RACI matrix to be approved by AHCCCS/Med-QUEST.

6.1.9 COMMUNICATION MANAGEMENT

Communication is essential to successful projects and clear communication vehicles must be established. The PMS Project Communication Management Plan, a subsidiary plan to this PMP, defines the communication requirements and provides the framework for managing and coordinating the PMS project deliverables and other communications. The plan addresses communicators, audiences, messages, communication channels, and feedback mechanisms to ensure that relevant, accurate, and consistent information is exchanged within the PMS project team and with and among AHCCCS/Med-QUEST and other PMS project stakeholders. This plan establishes standard communications and interactions among project team members and stakeholders, including reporting, meetings, escalation procedures, and action item resolution.

Adhering to communication goals and guiding principles is key to ensuring that communications are clear, consistent, and effective in delivering their message. The goals of the PMS project Communication Management Plan include the following:

- Communicate PMS project information to all stakeholders
- Ensure that communication roles and responsibilities are well understood
- Encourage trust and confidence in the information exchange
- Facilitate multiple modes of communication by soliciting, encouraging, and responding to feedback, questions, comments, and ideas
- Ensure that appropriate communication methods are used for the respective communication.

The PMS project Communication Management Plan identifies meetings, deliverables, action item tracking, and other methods of communication used by the PMS project team. These communication items are included in the Communication Matrix and are under configuration control as outlined in the PMS project Configuration Management Plan.

The Communication Management Plan defines the following:

- Communication requirements based on roles
- What information will be communicated
- How the information will be communicated
- When the information will be distributed
- Who does the communication
- Who receives the communication.

The Communication Management Plan serves as a guide for communications throughout the life of the PMS project contract and is updated as communication needs change. The plan identifies the roles of the stakeholders involved in the PMS project and includes a communications matrix that documents each type of communication, recipients, delivery method, frequency, format, and individuals responsible for delivery. The types of project communications documented in this matrix include the following:

- Meetings: Weekly, bi-weekly and monthly project status, and other meetings as they are established
- Project Management Materials: Schedule/WBS, issues log, risk report.

The Communication Management Plan is necessary to manage the project team and stakeholder expectations to prevent un-channeled communications and ensure timely and appropriate collection, generation, dissemination, and storage of information. The PMS project SharePoint site, where all documentation and meeting materials are stored and made accessible to PMS project team members, plays a vital role in dissemination, control, and tracking of internal program communications.

6.1.10 RISK MANAGEMENT

The purpose of risk management is to identify potential problems before they occur so that risk handling activities can be planned and invoked as needed across the life of the product or project to mitigate or eliminate adverse impacts on achieving project objectives. Risk management encompasses several processes, including planning for risk, identifying risk, analyzing risk, responding to risks, and monitoring and controlling risks. All risks will be logged in the PMS project risk register and managed throughout the project duration to decrease the probability of occurrence and impact of adverse risks. The PMS project team will perform the following activities to manage the project risks:

6.1.10.1 Risk Identification Techniques

There are multiple sources of risk. Identifying risks to the project involve recognizing existing conditions, activities, or potential decisions that may jeopardize the PMS project's success. Techniques that can be used to identify risks include formal or informal

risk assessment workshops, brainstorming, Delphi technique (expert consensus), and interviews. Potential sources of risks to the program include the following:

- Project scope creep
- Project schedule slippage
- Resource allocation changes
- Decrease in budget
- Increase in costs
- Significant changes to business requirements
- Baseline changes
- Unresolved issues
- Interdependencies among other projects
- Any other source that potentially impacts the project.

The PMS project team members are responsible for monitoring all aspects of the project to identify current or future risks. If a current or future risk is identified, the team member report the risk to the project manager and the team moves forward with analyzing the risk.

6.1.10.2 Risk Analysis

Once a risk is identified, the project manager then works with project staff to analyze the identified risk using a) qualitative analysis and, if able, b) quantitative analysis. The analysis includes a comprehensive evaluation of the potential impact of the risk on the program. The analysis will include, but not be limited to, an evaluation of the risks listed in the table below.

Field Name	Description
Probability	Qualitative risk analysis numeric factor used to weigh the probability that a risk will occur. (1–5)
Impact	Qualitative risk analysis numeric factor used to assess the impact the risk will cause if it occurs (1–5)
Risk Exposure	Qualitative risk analysis numeric factor used to assign to a risk with regard to magnitude based on probability and impact (Probability x Impact = Rating)

In performing qualitative risk analysis, the PMS project team will use the categories of risk impact shown in the table below.

Risk Impact	
5	Catastrophic
4	Critical
3	Serious
2	Marginal
1	Negligible

The project team will assess the probability of risk realization and assign a percentage using the Risk Probability shown in the table below as a guideline.

Risk Probability	
5	Near Certainty
4	Highly Likely
3	Likely
2	Unlikely
1	Remote

If deemed necessary by the project manager, a quantitative risk analysis is performed to assign quantitative values to impact and/or probability using quantitative models such as Expected Monetary Value, Sensitivity Analysis, or Monte Carlo Analysis.

Prioritize Risk

The project team will conduct a qualitative analysis of the risk by assessing the priority of the risk. Based on the project team's evaluation of the risk impact and probability, the risk is assigned a priority of High, Moderate, or Low. The risk exposure is a calculated value, where exposure equals the likelihood (probability) multiplied by the impact estimate. Risk exposure is a standard quantitative measure of risk and is used to rate the criticality of the risk and to compare risks to one another.

Risk Exposure	
High	12–25
Moderate	6–11
Low	1–5

For example, if a risk that is assessed to have an Impact of 3 due to the potential for a moderate slip in schedule was assessed to have a Probability of 4, then the risk would be assigned a Risk Level of High because 3 × 4 or 12.

6.1.10.3 Develop Mitigation and Contingency Plans

Based on the analysis and the severity of the risk, the project manager works with the project team to develop a mitigation plan that reduces the potential impact of the risk on the project. The mitigation plan includes the documented steps that will be taken to avoid realization of the risk. The goal of the mitigation plan is to develop an actionable approach for mitigating the risk so that it does not affect the project. A mitigation plan is required for all moderate and high risks. For low risks, development of a mitigation plan is based on the discretion of the project manager.

A contingency plan is required for high risks in case the risk is realized and becomes an issue. A contingency plan may be created for moderate risks at the discretion of the project manager.

Mitigation and contingency plans are recorded and monitored in the project's risk register.

6.1.10.4 Response Strategy

Risk response strategies are options and actions to reduce or eliminate threats or risks to the project, and include the following:

Mitigate Risk: Project staff have been assigned to implement mitigation strategies to proactively minimize the impact or probability of the risk.

Accept Risk: The customer and project team have made an informed and deliberate decision to accept the consequences and likelihood of the risk.

Avoid Risk: The project team decided to change its plan to eliminate the probability of the risk occurring or the impact of the risk if it does occur.

Transfer Risk: Ownership of the risk has been moved to another organizational element, such as an external entity or to the customer.

6.1.10.5 Monitor Risk

After a risk is identified and evaluated, the risk is moved into the monitor phase. During the monitor phase, the project team monitors the risk for any updates or new actionable approaches to mitigating the risk during a regularly scheduled meeting at an interval selected by the project manager. If a major change to a risk occurs between scheduled meetings, an ad hoc meeting is convened to address the risk immediately. During the monitor phase, the impact, priority, mitigation plan, contingency plan, and/or risk response strategy may require a change and/or additional analysis. The risk may become realized during this phase; if the risk is realized, the risk is converted to an issue and transferred to the issues log. See Section 6.13 for details about realized risks.

6.1.10.5 Close Risk

There are two instances where a risk can be closed, as follows:

Risk No Longer Impacts Project: If the risk was successfully mitigated, avoided, accepted, or transferred by the project team, then the risk no longer has a potential impact on the project and can be closed.

Risk Was Realized: If the project manager decides that the risk's impact on the project is no longer potential, but has become real, then the risk has been realized. If a risk is realized, it is converted to an issue and transferred to the issues log. Once the risk is converted to an issue, the risk is retired (closed) because it is no longer a risk.

6.1.10.6 Risk Register (Risk Log)

The PMS project risk register is stored on the project's internal SharePoint site.

6.1.11 CONFIGURATION MANAGEMENT

Configuration management (CM) for the PMS project is handled in accordance with the PMS Project Configuration Management Plan (CMP), a subsidiary plan to this PMP. The CMP details the handling and stewardship of the PMS project configuration items (CI) throughout the project's life cycle, including the deliverables list, software, and the storage of documents and files.

AHCCCS/Med-QUEST regularly reviews proposed changes, solicits feedback from all relevant stakeholders, and serves as a central point to approve or reject the incorporation of changes. We will ensure all relevant stakeholders review and approve change reviews and that all relevant stakeholders are informed of the change management process and the status of change requests (CR).

For all changes to the PMS environment, we will perform an internal review of change plans and potential impacts. Once a change is approved by our quality assurance manager, we document the proposed change; the rationale for and impact of the change; and develop implementation, testing, and back-out plans. We present the proposed changes to AHCCCS/Med-QUEST for approval and include approved changes in the weekly change coordination meeting and calendar of planned changes. We enhance the change control process by automating the approval process for low-risk changes using Jira, allowing the weekly meeting to focus on medium- to high-risk changes in the PMS environment.

The CMP establishes the administrative direction and surveillance for the management of CIs associated with the PMS project and defines the project's structure and methods for the following activities:

- Identifying deliverables, work products, and baselines (released documents) that are subject to configuration control
- Approving and rejecting proposed changes to CIs
- Tracking the status of and reporting changes to the configuration data
- Auditing CIs to ensure that controlled items meet their requirements and are correctly documented.

The CMP outlines the objectives of the CM practices, which are applied consistently and uniformly to all PMS project CIs.

6.1.12 ISSUE MANAGEMENT

Issues can occur on a project through multiple sources, and can originate as an unforeseen item, or as a result of a realized project risk. The PMS project issue management approach includes steps to proactively manage project issues as they occur.

6.1.12.1 Identify Issue

Once an issue is identified, the project manager ensures it is recorded in the issues log on the project SharePoint site and that the following key information is captured at the time of entry:

- Issue description that includes details about the issue event and the potential impact
- Associated risk, if applicable, for traceability.

6.1.12.2 Prioritize Issue

The project team assesses the issue and categorizes it to identify the project area that it directly impacts. Parameters for evaluating, categorizing, and prioritizing issues include the following:

- Issue Category: Defined categories to organize and track issues based on project activities and/or other factors
- Issue Impact: Assigned numerical value to indicate the potential severity of the impact
- Priority: Derived from impact on a scale of High, Medium, and Low.

An issue owner is assigned. The project manager works with the issue owner to document other key information to facilitate with issue resolution.

6.1.12.3 Corrective Action Planning

Once an issue has been assessed and prioritized, the project team develops a corrective action plan to resolve the issue. The corrective action plan is documented along with the issue in the issues log.

A target resolution date is determined to set a deadline for resolving the issue.

The status of the issue is maintained for identified issues to track progress toward resolution.

6.1.12.4 Monitor and Resolve Issue

After a plan of action to resolve the issue has been developed, the project manager monitors the execution of each step in the identified corrective action plan.

The top project issues are reported and communicated to the project team, AHCCCS/Med-QUEST, and other stakeholders through project status reports, during project status discussions, and via other means (e.g., meetings).

6.1.12.5 Issues List (Issue Log)

The issues list is maintained as a separate document and stored on the PMS project internal SharePoint site.

6.1.13 RECORDS MANAGEMENT

All project materials are stored on the NewWave PMS project SharePoint site.

See the PMS project Configuration Management Plan for details of our records management process for this project.

6.1.14 ACQUISITION STRATEGY

The PMS project team follows NewWave's supplier agreement management procedure for acquiring equipment and services, as well as subcontractors. The process includes a formal selection process and ongoing monitoring and evaluation.

6.1.14.1 Subcontractor Management

The Provider Management System project team includes one subcontractor: IBM Watson Health. NewWave, as prime contractor, manages all program aspects, including managing subcontractors across the contract.

On contract award, NewWave will develop a detailed Subcontractor Management Plan—as a subsidiary plan to this PMP—that details the following principles and practices. NewWave is responsible for all deliverables and the activities of our entire team. We integrate subcontractors fully into the planning, scheduling, and reporting requirements for each task. Our task monitoring process and comprehensive reviews, reports, and metrics enable us to isolate a subcontractor's project contributions and its impact on meeting assigned task requirements. NewWave has executed a teaming agreement with our subcontractor; and the subcontractor agreement will be in place on contract award.

The subcontractor management process is based on the following:

Structure: The team's organization is straightforward; it provides a single point of leadership and clear lines of authority. All employees, regardless of company affiliation, function as members of one integrated team. Subcontractor roles are clear and work share is well defined.

Agreements: NewWave contracts department staff members draft all subcontractor agreements and monitor adherence to all contractual terms. In all subcontracting agreements, NewWave spells out, in detail, the procedures for prompt invoicing and payment, the promotion of fairness in the division of work share, general communication, and conflict resolution. An established set of standards ensures a common understanding of purpose and consistency of action.

Leadership: The project manager has direct oversight of all subcontractors and regularly reviews team member performance. He also serves as the primary point of contact for subcontractors.

General Communication: Communication procedures take several forms. We establish rapid and efficient intra-team communication among all team members. The guidelines regarding communications with the customer and other external agencies are established in the Communications Management Plan of the PMP. The team speaks with a common voice when answering questions raised by the customer, but, more important, such guidelines ensure the customer gets the right answer from someone authorized to provide it.

Quality Control: To ensure service quality and compliance, we use an established set of standards and processes with which all team members agree to conform. The principles of these two important elements are established first in the subcontracting agreements, and, finally, in the Quality Management Plan. NewWave's standard project management processes and risk mitigation strategies are used to measure subcontractor performance.

Conflict Resolution: In every business relationship, issues and problems arise that require immediate resolution and attention. Based on NewWave's established communication processes and procedures and on open communications with AHCCCS/Med-QUEST and other stakeholders, NewWave identifies and resolves issues quickly at the lowest organizational level possible.

6.1.15 SOFTWARE PROCESS IMPROVEMENT (SPI)

Team NewWave for the PMS project is committed to process improvement. NewWave's process framework aligns with industry best practices, including CMMI for Services, CMMI for Development, PMBOK, and the CMS XLC. We continually review and improve these processes to ensure successful product and service delivery. This framework provides a common understanding of process improvement and the PMS project management methodology. The QA and PMO offices conduct regular audits and reviews of project processes and products to ensure compliance with those standards and customer expectations. We provide details on our quality control and quality assurance processes in the project's Quality Management Plan.

NewWave is committed to achieving customer satisfaction and high-quality products and services and thus supports continuous process improvement by implementing industry best practices as they apply to the needs of our projects and customers. The Vice President of Corporate Compliance leads these efforts and coordinates resources and tasks among projects and relevant stakeholders.

The PMS project will hold lessons learned sessions to gain an understanding of what is going well with the project and where there are opportunities for improvement. The team will conduct lessons learned reviews at a minimum at the end of each release. Team NewWave also will hold sprint retrospectives at the end of each sprint.

6.1.15.1 CMMI

NewWave was reappraised at CMMI Maturity Level 3 for Development in December 2015 and is scheduled to be appraised at CMMI Maturity Level 4 for Development in late third quarter of 2018. NewWave was appraised at CMMI Maturity Level 4 for Services in January 2018.

The NewWave Process Improvement Plan defines the strategy and activities for implementing CMMI-appraised best practices across the NewWave service projects. This plan establishes objectives, responsibilities, activities, resources, and tools to monitor progress and facilitate successful execution of this plan. The objectives of this plan are as follows:

- Undergo a successful CMMI-DEV ML4 Standard CMMI Assessment Method for Process Improvement A (SCAMPI-A) appraisal before fourth quarter 2018
- Fine-tune and/or develop processes and best practices
- Maintain a CMMI-SVC ML4–rated metrics program
- Maintain a CMMI-DEV ML4–rated audit process
- Provide for continuous process improvement.

6.1.16 SECURITY

The PMS project's infrastructure meets Arizona Security Controls 2017 and we will monitor real-time compliance and vulnerability. Remediations will be schedule according to security policy and change control policy.

We will deploy Splunk, an advanced log aggregation and monitoring tool. NewWave will configure Splunk to use machine learning to identify usage anomalies, which can consist of a single action or a series of actions. The NewWave security analyst will review the logs and report any incidents of misuse. Splunk will maintain logs of all actions taken by system users and maintain them for the life of the contract, enabling us to produce reports of any actions taken by users as required.

The solution also keeps a database log of users' authenticated access to the system as well as unauthorized attempts to access information within the application. These database tables can be queried and reported to appropriate staff.

System changes are captured by an audit feature within the solution, which can be turned on for specific database tables. Once turned on, changes made to data are captured along with a timestamp and the username of the user initiating the change.

All systems display a security banner with either the NIST-compliant wording or other wording as the state requires.

All critical vulnerabilities are patched within 3 business days; major vulnerabilities are patched within 10 days. The team continually monitors the environment and plans patches via a detailed change control process.
All users will use a unique account. All accounts used by system will be monitored for usage by a person rather than the system.
Team NewWave will provide, within 12 hours of any security Incident, an email that includes details of the type, scope, and impact of the incident along with any actions already taken or planned.

Our solution has a built-in mechanism to support both authentication and authorization regarding application security. The built-in authentication can be turned off in favor of a configurable integration with an LDAP 3.0 directory for user authentication. This is a

common requirement on many projects to integrate with an external authentication source and Team NewWave will ensure the authentication of users against the desired LDAP directory.

The solution offers a robust and configurable role-based authorization control (RBAC) mechanism. Once authenticated via the external LDAP source, the application enforces authorization through the use of assigned roles and function and data identifiers. Users may only access functions and data that are explicitly authorized by the administrator. Multiple roles may be created using our configurable administration console. Using this mechanism, users are assigned roles that correspond to their duties with the appropriate level of access.

Our solution has the capability to enable multiple forms of system- and business-level auditing, including the following:

- Database Table Auditing
- Business Function Auditing
- Security Auditing
- Workflow Activity Auditing.

Database auditing enables the system to capture the actions carried out on information held in the solution database tables, including the user ID, table name, date and time, and other pertinent information.

Security auditing enables the system to capture authentication attempts as well as authorization failures. All auditing information is stored in database tables and can be easily extracted for reporting purposes.

Our solution enforces a RBAC model for authorized access. This model, when applied to individual data fields on a user screen, automatically checks the logged-in user's security role against the data elements on the screen. If the user does not have the assigned security identifiers, the screen displays a set of asterisks (*) instead of the real data value, effectively redacting records against unauthorized access.

All team members receive annual HIPPA security training and we will provide proof of completion for each staff member on request.

6.1.17 Privacy

Internal project artifacts created during the PMS project will be available through a secure SharePoint collaborative site to which access can be granted on a case-by-case basis. The type of information generated during the PMS project and stored on the SharePoint site does not include personally identifiable information (PII), tax identifiable information (TII), or other highly confidential material.

Some information may be private. In cases where privacy is required, artifacts and information are secured on the collaborative SharePoint site in a manner that restricts access to only the intended audience. AHCCCS/Med-QUEST will provide guidance regarding what information is restricted to which audience. Where access questions arise, AHCCCS/Med-QUEST will be the arbiter of access rights.

All data are encrypted at rest on the physical hardware. All databases containing PHI and PII are encrypted at the software layer as well.

6.1.18 Business Continuity

Team NewWave ensures continuity of services in the event of an interruption of services by implementing the Organizational Business Continuity (BCON) Plan. As a component of this plan, the PMS project created a project-level BCON that defines the information, tasks, procedures, and documentation necessary to facilitate decision-making and timely response to disruption of normal business operations. The PMS project works closely with NewWave's Infrastructure and Security Teams to prioritize systems and necessary operations, define the business impacts of service interruptions, and designate emergency response teams to ensure continuity of leadership, governance, and management of business operations and services to the customer until full operations can be restored.

6.1.19 Compliance Related Training

NewWave requires each team member to complete the following training:

- Security
- Health Insurance Portability and Accountability Act (HIPAA)
- Ethics

- Capability Maturity Model Integration (CMMI) Overview

APPENDIX I: RECORD OF CHANGES

Version Number	Date	Author/Owner	Description of Change

APPENDIX II: PMP ACRONYMS LIST

Acronym	Literal Translation
AHCCCS	Arizona Health Care Cost Containment System Administration
CM	Configuration Management
CMMI	Capability Maturity Model Integration
EVM	Earned Value Management
HIPAA	Health Insurance Portability and Accountability Act
Med-QUEST	Hawaii Medicaid Program
MCO	Managed Care Organization
ORR	Operational Readiness Review
PII	Personally Identifiable Information
PMP	Project Management Plan
PMBOK	Project Management Body of Knowledge
SPIP	Software Process Improvement Plan
TII	Tax Identifiable Information
WBS	Work Breakdown Structure

APPENDIX III: GLOSSARY

Term	Definition
Records Management	The planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition to achieve adequate and proper documentation of the policies and transactions of the federal government and effective and economical management of agency operations (44 U.S.C. 2901 [2]).
Work Breakdown Structure (WBS)	A deliverables-oriented group of project components that organizes and defines the total scope of the project; work not in the WBS is outside the scope of the project. A WBS is normally presented in chart form. Each descending level represents an increasingly detailed description of the project deliverables.

APPENDIX IV: REFERENCED DOCUMENTS

Document Name	Document Location and/or URL	Issuance Date

APPENDIX V: PMP APPROVALS

The undersigned acknowledge that they have reviewed the Project Management Plan and agree with the information presented within this document. Changes to this Project Management Plan will be coordinated with, and approved by, the undersigned, or their designated representatives.

Signature: _____ Date: _____

Print Name: _____

Title: _____

Role: _____

Signature: _____ Date: _____

Print Name: _____

Title: _____

Role: _____

Signature: _____ Date: _____

Print Name: _____

Title: _____

Role: _____

APPENDIX VI: ADDITIONAL APPENDICES

APPENDIX C: PROJECT WORK PLAN TASK LIST

ID	WBS	Task Name	Duration	Start	Finish
1	1	Provider Management System	267 days?	Sat 9/1/18	Tue 9/17/19
2	1.1	Contract Award	0 days	Sat 9/1/18	Sat 9/1/18
3	1.2	Execute Sub-contract agreements	5 days	Mon 9/3/18	Fri 9/7/18
4	1.3	First 12 Months	267 days?	Mon 9/3/18	Tue 9/17/19
5	1.3.1	Contract Kickoff Meeting	112 days	Mon 9/10/18	Thu 2/14/19
6	1.3.1.1	Kickoff Meeting Prepatory Activities	4 days	Mon 9/3/18	Thu 9/6/18
7	1.3.1.2	Kickoff Meeting Agenda	2 days	Wed 9/5/18	Thu 9/6/18
8	1.3.1.3	Conduct Kickoff Meeting	1 day	Fri 9/7/18	Fri 9/7/18
9	1.3.2	Planning Phase	267 days	Mon 9/3/18	Tue 9/17/19
10	1.3.2.1	Joint Operating Agreements	8 days	Mon 9/3/18	Wed 9/12/18
14	1.3.2.2	Project Management Plan	9 days	Mon 9/3/18	Thu 9/13/18
19	1.3.2.3	Project Work Plan (PWP)	9 days	Mon 9/3/18	Thu 9/13/18
24	1.3.2.4	Communications Plan	13 days	Mon 9/10/18	Wed 9/26/18
29	1.3.2.5	Risk Management Plan	9 days	Mon 9/10/18	Thu 9/20/18
34	1.3.2.6	Isue Management Plan	9 days	Mon 9/10/18	Thu 9/20/18
39	1.3.2.7	Configuration/Change Management Plan	9 days	Fri 9/21/18	Wed 10/3/18
44	1.3.2.8	Staffing Management Plan	9 days	Fri 9/21/18	Wed 10/3/18
49	1.3.2.9	Quality Management Plan	9 days	Fri 9/21/18	Wed 10/3/18
54	1.3.2.10	Develop Application Roadmap	13 days	Mon 9/10/18	Wed 9/26/18
60	1.3.2.11	Software Product 508 Compliancy Checklist/VPAT	14 days	Thu 9/27/18	Tue 10/16/18
65	1.3.2.12	Reports	267 days	Mon 9/3/18	Tue 9/17/19
66	1.3.2.12.1	Staff Roster and Organization Chart	5 days	Mon 9/3/18	Fri 9/7/18
68	1.3.2.12.2	Meetings and Meeting Support	180 days	Fri 9/7/18	Mon 5/20/19
71	1.3.2.12.3	Management Reviews	180 days	Fri 9/7/18	Mon 5/20/19
74	1.3.2.12.4	Dashboard and Status Reports Templates	180 days	Fri 9/7/18	Mon 5/20/19
76	1.3.2.12.5	Monthly/Weekly Status Reports	258 days	Fri 9/14/18	Tue 9/17/19
155	1.3.2.12.6	Root Cause Analysis (RCA) Report	258 days	Fri 9/7/18	Tue 9/10/19
157	1.3.2.13	Deliverables	262 days	Mon 9/3/18	Tue 9/10/19
158	1.3.2.13.1	1. Project Management (Weekly and on-going as defined)	251 days	Fri 9/14/18	Fri 9/6/19
159	1.3.2.13.1.1	a. Weekly IT Planning Session involvement	251 days	Fri 9/14/18	Fri 9/6/19
160	1.3.2.13.1.2	b. Develop milestone schedule (weekly, monthly and quarterly)	251 days	Fri 9/14/18	Fri 9/6/19
161	1.3.2.13.1.3	c. Contributions to the overall project plan maintained by AHCCCS/Med-QUEST	251 days	Fri 9/14/18	Fri 9/6/19
162	1.3.2.13.2	2. Business process analysis and system requirements document (Deliverable within 30 days from contract implementation)	23 days	Mon 9/3/18	Wed 10/3/18
163	1.3.2.13.2.1	a. Baseline Review (includes Project Start-Up along with Administrative and Baseline Reviews)	23 days	Mon 9/3/18	Wed 10/3/18
164	1.3.2.13.2.2	b. System Security Assessment	23 days	Mon 9/3/18	Wed 10/3/18
165	1.3.2.13.2.3	c. Data/System Security Plan	23 days	Mon 9/3/18	Wed 10/3/18
166	1.3.2.13.2.4	d. Data Use/Exchange Interconnection Security Agreement	23 days	Mon 9/3/18	Wed 10/3/18
167	1.3.2.13.2.5	e. Risk Assessment Plan	23 days	Mon 9/3/18	Wed 10/3/18
168	1.3.2.13.2.6	f. Complete Privacy Impact Analysis (PIA)	23 days	Mon 9/3/18	Wed 10/3/18
169	1.3.2.13.3	3. System Design (Deliverable 60-90 days from contract implementation agreed upon between AHCCCS/Med-QUEST and Contractor)	38 days	Mon 9/3/18	Wed 10/24/18
170	1.3.2.13.3.1	a. Interface Design/Control document. COTS to mainframe interface design.	38 days	Mon 9/3/18	Wed 10/24/18
175	1.3.2.13.3.2	b. Architecture walkthrough and requirements analysis	37 days	Mon 9/3/18	Tue 10/23/18
176	1.3.2.13.3.2.1	Develop System Design Document	37 days	Mon 9/3/18	Tue 10/23/18
180	1.3.2.13.3.3	c. Database design	30 days	Mon 9/3/18	Fri 10/12/18
181	1.3.2.13.3.4	d. Detailed Design Review (includes Preliminary and Detailed Design Reviews)	30 days	Mon 9/3/18	Fri 10/12/18
182	1.3.2.13.3.5	e. Final Detailed Design Review	30 days	Mon 9/3/18	Fri 10/12/18
183	1.3.2.13.3.6	f. Data conversion analysis and conversion plan	30 days	Mon 9/3/18	Fri 10/12/18
184	1.3.2.13.4	4. Development (Begin date NLT 120 days from contract implementation date)	3 days	Thu 5/9/19	Tue 5/14/19

Page 1

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

ID	WBS	Task Name	Duration	Start	Finish
185	1.3.2.13.4.1	a. Portals, for state worker access, Provider enrollment/registration and reporting	1 day	Mon 5/13/19	Tue 5/14/19
186	1.3.2.13.4.2	b. User training plan (knowledge transfer, desktop manuals, on-site training)	1 day	Thu 5/9/19	Fri 5/10/19
187	1.3.2.13.4.3	c. Contingency Plan/Recovery Plan	1 day	Thu 5/9/19	Fri 5/10/19
188	**1.3.2.13.5**	**5. Testing and Evaluation (Begin Date NLT 160 days from contract implementation date)**	**149.5 days**	**Mon 10/15/18**	**Tue 5/14/19**
189	1.3.2.13.5.1	a. Test plan for functional, integration, system, regression and user acceptance testing	1 day	Mon 10/15/18	Mon 10/15/18
190	1.3.2.13.5.2	b. Validation of test reporting	1 day	Mon 5/13/19	Tue 5/14/19
191	1.3.2.13.5.3	c. Error reporting and remediation planning for test stages	1 day	Mon 10/15/18	Mon 10/15/18
192	**1.3.2.13.6**	**6. Implementation (Deliverable 10 days from Integrated Testing Acceptance)**	**1 day**	**Mon 9/3/18**	**Mon 9/3/18**
193	1.3.2.13.6.1	a. Implementation/Roll out plan to include dashboard reporting.	1 day	Mon 9/3/18	Mon 9/3/18
194	1.3.2.13.6.2	b. Validated of production reports	1 day	Mon 9/3/18	Mon 9/3/18
195	1.3.2.13.6.3	c. Ongoing error reporting	1 day	Mon 9/3/18	Mon 9/3/18
196	1.3.2.13.6.4	d. SLA agreements	1 day	Mon 9/3/18	Mon 9/3/18
197	**1.3.2.13.7**	**7. Post Implementation (Deliverable 60 days from Integrated Testing Acceptance)**	**1 day**	**Mon 9/3/18**	**Mon 9/3/18**
198	1.3.2.13.7.1	a. Post implementation plan for both AHCCCS/Med-Quest	1 day	Mon 9/3/18	Mon 9/3/18
199	1.3.2.13.7.2	b. Post implementation documentation delivery	1 day	Mon 9/3/18	Mon 9/3/18
200	1.3.2.13.7.3	c. Post implementation support/maintenance plan	1 day	Mon 9/3/18	Mon 9/3/18
201	1.3.2.13.7.4	d. Error reporting and remediation planning	1 day	Mon 9/3/18	Mon 9/3/18
202	**1.3.2.13.8**	**8. IV&V Coordination and Reporting (This is an ongoing requirement from date of contraction implementation through System Certification by CMS. Targeted end date is December 2019)**	**257 days**	**Mon 9/10/18**	**Tue 9/10/19**
203	1.3.2.13.8.1	a. Timely response to all request from IV&V	257 days	Mon 9/10/18	Tue 9/10/19
204	1.3.2.13.8.2	b. Quarterly reporting	257 days	Mon 9/10/18	Tue 9/10/19
205	1.3.2.13.8.3	c. Milestone reporting	257 days	Mon 9/10/18	Tue 9/10/19
206	1.3.2.13.8.4	Develop and deliver a plan for CMS Certification	30 days	Mon 9/10/18	Fri 10/19/18
207	**1.3.2.14**	**Network Connectivity & Configuration**	**260 days**	**Mon 9/3/18**	**Fri 9/6/19**
210	**1.3.3**	**System Security**	**262 days**	**Mon 9/3/18**	**Tue 9/10/19**
211	1.3.3.1	Ensure compliance with AHCCCS/Med-QUEST security policies and operations	262 days	Mon 9/3/18	Tue 9/10/19
212	1.3.3.2	Maintain security architecture	262 days	Mon 9/3/18	Tue 9/10/19
213	1.3.3.3	Provide Security Awareness Training	262 days	Mon 9/3/18	Tue 9/10/19
214	1.3.3.4	Perform security monitoring and evaluation	262 days	Mon 9/3/18	Tue 9/10/19
215	**1.3.3.5**	**System Security Plan (SSP)**	**24 days**	**Mon 9/3/18**	**Thu 10/4/18**
218	**1.3.3.6**	**Contingency Plan (CP)**	**26 days**	**Mon 9/3/18**	**Mon 10/8/18**
222	**1.3.3.7**	**Contingency Plan (CP) Tabletop Test After Action Report (AAR)**	**3 days**	**Thu 5/30/19**	**Tue 6/4/19**
226	**1.3.3.8**	**Plan of Action and Milestones (POA&M) as required**	**1 day**	**Mon 9/3/18**	**Mon 9/3/18**
228	**1.3.3.9**	**Corrective Action Plan (CAP) as required**	**1 day**	**Mon 9/3/18**	**Mon 9/3/18**
230	**1.3.3.10**	**Information Security (IS) Risk Assessment (RA)**	**24 days**	**Mon 9/3/18**	**Thu 10/4/18**
234	**1.3.3.11**	**Background Investigation Status Report as required**	**1 day**	**Mon 9/3/18**	**Mon 9/3/18**
236	**1.3.3.12**	**Risk Vulnerability Assessment (RVA)**	**24 days**	**Mon 6/3/19**	**Fri 7/5/19**
238					
239	**1.3.4**	**PMS Implementation**	**234 days**	**Mon 9/3/18**	**Wed 7/31/19**
240	**1.3.4.1**	**Sprint 0**	**25 days**	**Mon 9/10/18**	**Fri 10/12/18**
241	1.3.4.1.1	Develop prioritized Epics	10 days	Mon 9/10/18	Fri 9/21/18
242	1.3.4.1.2	Developed prioritized Features	15 days	Mon 9/10/18	Fri 9/28/18
243	1.3.4.1.3	Develop prioritized user stories for Sprints	18 days	Mon 9/10/18	Wed 10/3/18
244	1.3.4.1.4	Conduct JAD Sessions	18 days	Mon 9/10/18	Wed 10/3/18
245	1.3.4.1.5	Develop and deliver UAT Test Plan	5 days	Mon 9/10/18	Fri 9/14/18
246	1.3.4.1.6	Establish and groom Product backlog	2 days	Thu 10/4/18	Fri 10/5/18
247	**1.3.4.1.7**	**Implementation Schedule**	**10 days**	**Mon 10/1/18**	**Fri 10/12/18**

Page 2

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

ID	WBS	Task Name	Duration	Start	Finish
248	1.3.4.1.7.1	Draft Epic, Feature and Sprint Schedules	4 days	Mon 10/1/18	Thu 10/4/18
249	1.3.4.1.7.2	Conduct internal review of Schedules	2 days	Fri 10/5/18	Mon 10/8/18
250	1.3.4.1.7.3	Incorporate internal feedback into Schedules	1 day	Tue 10/9/18	Tue 10/9/18
251	1.3.4.1.7.4	Review and Baseline Schedules with AHCCS/Med-QUEST	2 days	Wed 10/10/18	Thu 10/11/18
252	1.3.4.1.7.5	Submit Epic, Feature and Sprint Schedules to AHCCCS/Med-QUEST	1 day	Fri 10/12/18	Fri 10/12/18
253	1.3.4.2	Milestone: Planning Sprint 0 Complete	0 days	Fri 10/12/18	Fri 10/12/18
254	**1.3.4.3**	**Sprint 1**	**10 days**	**Mon 10/15/18**	**Fri 10/26/18**
255	1.3.4.3.1	Sprint Planning	0.5 days	Mon 10/15/18	Mon 10/15/18
256	1.3.4.3.2	Discovery (Develop User, business and system requirements)	10 days	Mon 10/15/18	Fri 10/26/18
257	1.3.4.3.3	Design (Architect, software components/modules, interfaces and/or database)	10 days	Mon 10/15/18	Fri 10/26/18
258	1.3.4.3.4	Conduct JAD Sessions	10 days	Mon 10/15/18	Fri 10/26/18
259	1.3.4.3.5	Implement Sprint Tasks	10 days	Mon 10/15/18	Fri 10/26/18
260	1.3.4.3.6	System Integration Testing	10 days	Mon 10/15/18	Fri 10/26/18
261	1.3.4.3.7	Sprint Review and Retrospective	0.5 days	Fri 10/26/18	Fri 10/26/18
262	1.3.4.4	Milestone: Sprint 1 Complete	0 days	Fri 10/26/18	Fri 10/26/18
263	**1.3.4.5**	**Sprint 2**	**10 days**	**Mon 10/29/18**	**Fri 11/9/18**
264	1.3.4.5.1	Sprint Planning	0.5 days	Mon 10/29/18	Mon 10/29/18
265	1.3.4.5.2	Discovery (Develop User, business and system requirements)	10 days	Mon 10/29/18	Fri 11/9/18
266	1.3.4.5.3	Design (Architect, software components/modules, interfaces and/or database)	10 days	Mon 10/29/18	Fri 11/9/18
267	1.3.4.5.4	Conduct JAD Sessions	10 days	Mon 10/29/18	Fri 11/9/18
268	1.3.4.5.5	Implement Sprint Tasks	10 days	Mon 10/29/18	Fri 11/9/18
269	1.3.4.5.6	System Integration Testing	10 days	Mon 10/29/18	Fri 11/9/18
270	1.3.4.5.7	Sprint Review and Retrospective	0.5 days	Fri 11/9/18	Fri 11/9/18
271	1.3.4.6	Milestone: Sprint 2 Complete	0 days	Fri 11/9/18	Fri 11/9/18
272	**1.3.4.7**	**Sprint 3**	**11 days**	**Mon 11/12/18**	**Mon 11/26/18**
273	1.3.4.7.1	Sprint Planning	0.5 days	Mon 11/12/18	Mon 11/12/18
274	1.3.4.7.2	Discovery (Develop User, business and system requirements)	10 days	Mon 11/12/18	Mon 11/26/18
275	1.3.4.7.3	Design (Architect, software components/modules, interfaces and/or database)	10 days	Mon 11/12/18	Mon 11/26/18
276	1.3.4.7.4	Conduct JAD Sessions	10 days	Mon 11/12/18	Mon 11/26/18
277	1.3.4.7.5	Implement Sprint Tasks	10 days	Mon 11/12/18	Mon 11/26/18
278	1.3.4.7.6	System Integration Testing	10 days	Mon 11/12/18	Mon 11/26/18
279	1.3.4.7.7	Sprint Review and Retrospective	0.5 days	Mon 11/26/18	Mon 11/26/18
280	1.3.4.8	Milestone: Sprint 3 Complete	0 days	Mon 11/26/18	Mon 11/26/18
281	**1.3.4.9**	**Perform Epic Business Review 1 with Stakeholders**	**2 days**	**Tue 11/27/18**	**Wed 11/28/18**
282	1.3.4.9.1	Provide User Stories from previous Sprints for End User usage	1 day	Tue 11/27/18	Tue 11/27/18
283	1.3.4.9.2	Provide simulated data for database and interfaces (as required)	1 day	Tue 11/27/18	Tue 11/27/18
284	1.3.4.9.3	Conduct Review of all User Stories and collect feedback	1 day	Wed 11/28/18	Wed 11/28/18
285	**1.3.4.10**	**Sprint 4**	**11 days**	**Wed 11/28/18**	**Thu 12/13/18**
293	1.3.4.11	Milestone: Sprint 4 Complete	0 days	Wed 11/28/18	Wed 11/28/18
294	**1.3.4.12**	**Sprint 5**	**10.5 days**	**Fri 11/30/18**	**Fri 12/14/18**
302	1.3.4.13	Milestone: Sprint 5 Complete	0 days	Thu 12/13/18	Thu 12/13/18
303	**1.3.4.14**	**Sprint 6**	**10.5 days**	**Mon 12/17/18**	**Mon 12/31/18**
311	1.3.4.15	Milestone: Sprint 6 Complete	0 days	Fri 12/28/18	Fri 12/28/18
312	**1.3.4.16**	**Perform Epic Business Review 2 with Stakeholders**	**2 days**	**Mon 12/31/18**	**Wed 1/2/19**
313	1.3.4.16.1	Provide User Stories from previous Sprints for End User usage	1 day	Mon 12/31/18	Mon 12/31/18
314	1.3.4.16.2	Provide simulated data for database and interfaces (as required)	1 day	Mon 12/31/18	Mon 12/31/18
315	1.3.4.16.3	Conduct Review of all User Stories and collect feedback	1 day	Wed 1/2/19	Wed 1/2/19
316	**1.3.4.17**	**Sprint 7**	**10.5 days**	**Thu 1/3/19**	**Thu 1/17/19**
324	1.3.4.18	Milestone: Sprint 7 Complete	0 days	Wed 1/16/19	Wed 1/16/19

Page 3

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

ID	WBS	Task Name	Duration	Start	Finish
325	**1.3.4.19**	**Sprint 8**	**10.5 days**	**Fri 1/18/19**	**Mon 2/4/19**
333	1.3.4.20	Milestone: Sprint 8 Complete	0 days	Fri 2/1/19	Fri 2/1/19
334	1.3.4.21	**Begin User Acceptance Testing (UAT)**	15 days	Mon 1/28/19	Fri 2/15/19
335	**1.3.4.22**	**Sprint 9**	**10.5 days**	**Tue 2/5/19**	**Tue 2/19/19**
343	1.3.4.23	Milestone: Sprint 9 Complete	0 days	Mon 2/18/19	Mon 2/18/19
344	**1.3.4.24**	**Perform Epic Business Review 3 with Stakeholders**	**2 days**	**Tue 2/19/19**	**Wed 2/20/19**
345	1.3.4.24.1	Provide User Stories from previous Sprints for End User usage	1 day	Tue 2/19/19	Tue 2/19/19
346	1.3.4.24.2	Provide simulated data for database and interfaces (as required)	1 day	Tue 2/19/19	Tue 2/19/19
347	1.3.4.24.3	Conduct Review of all User Stories and collect feedback	1 day	Wed 2/20/19	Wed 2/20/19
348					
349	**1.3.5**	**AHCCCS Milestone Gate Reviews**	**35 days**	**Tue 2/5/19**	**Mon 3/25/19**
350	1.3.5.1	Perform Penetration Test and provide results to AHCCCS and Med-QUEST	5 days	Tue 2/19/19	Mon 2/25/19
351	1.3.5.2	Develop Operational Readiness Review (ORR) Plan	5 days	Tue 2/5/19	Mon 2/11/19
352	1.3.5.3	Provide ORR Plan for AHCCCS/Med-QUEST Review and Approval	0 days	Mon 2/11/19	Mon 2/11/19
353	1.3.5.4	Prepare for ORR	10 days	Tue 2/12/19	Mon 2/25/19
354	1.3.5.5	Conduct Operational Readiness Review (ORR)	0 days	Mon 2/25/19	Mon 2/25/19
355	1.3.5.6	Prepare for PRR	10 days	Tue 2/26/19	Mon 3/11/19
356	1.3.5.7	Production Readiness Review (PRR) approval to Go Live	0 days	Mon 3/11/19	Mon 3/11/19
357	1.3.5.8	Prepare for Production Go Live	9 days	Tue 3/12/19	Fri 3/22/19
358	1.3.5.9	Go Live	0 days	Mon 3/25/19	Mon 3/25/19
359					
360	**1.3.6**	**HI Sprint 1**	**10 days**	**Wed 3/27/19**	**Tue 4/9/19**
368	1.3.7	Milestone: Sprint 1 Complete	0 days	Tue 4/9/19	Tue 4/9/19
369	**1.3.8**	**HI Sprint 2**	**10 days**	**Wed 4/10/19**	**Tue 4/23/19**
377	1.3.9	Milestone: Sprint 2 Complete	0 days	Tue 4/23/19	Tue 4/23/19
378	1.3.10	**Begin User Acceptance Testing (UAT)**	1 day?	Wed 4/17/19	Wed 4/17/19
379	**1.3.11**	**HI Sprint 3**	**10.5 days**	**Thu 4/25/19**	**Thu 5/9/19**
387	1.3.12	Milestone: Sprint 3 Complete	0 days	Thu 5/9/19	Thu 5/9/19
388	**1.3.13**	**Perform Epic Business Review 1 with Stakeholders**	**2 days**	**Thu 5/9/19**	**Mon 5/13/19**
389	1.3.13.1	Provide User Stories from previous Sprints for End User usage	1 day	Thu 5/9/19	Fri 5/10/19
390	1.3.13.2	Provide simulated data for database and interfaces (as required)	1 day	Thu 5/9/19	Fri 5/10/19
391	1.3.13.3	Conduct Review of all User Stories and collect feedback	1 day	Fri 5/10/19	Mon 5/13/19
392					
393	**1.3.14**	**HI Milestone Gate Reviews**	**26 days**	**Tue 4/23/19**	**Thu 5/30/19**
394	1.3.14.1	Develop Operational Readiness Review (ORR) Plan	6 days	Tue 4/23/19	Wed 5/1/19
395	1.3.14.2	Provide ORR Plan for AHCCCS/Med-QUEST Review and Approval	0 days	Wed 5/1/19	Wed 5/1/19
396	1.3.14.3	Prepare for ORR	5 days	Wed 5/1/19	Wed 5/8/19
397	1.3.14.4	Conduct Operational Readiness Review (ORR)	0 days	Wed 5/8/19	Wed 5/8/19
398	1.3.14.5	Prepare for PRR	5 days	Wed 5/8/19	Wed 5/15/19
399	1.3.14.6	Production Readiness Review approval to Go Live	0 days	Thu 5/16/19	Thu 5/16/19
400	1.3.14.7	Prepare for Production Go Live	10 days	Wed 5/15/19	Thu 5/30/19
401	1.3.14.8	Go Live	0 days	Thu 5/30/19	Thu 5/30/19
402					
403	**1.3.15**	**PMS Operations**	**110 days**	**Tue 3/26/19**	**Wed 8/28/19**
404	1.3.15.1	Project Management	110 days	Tue 3/26/19	Wed 8/28/19
405	1.3.15.2	Operations Monitoring & Reporting	110 days	Tue 3/26/19	Wed 8/28/19
406	1.3.15.3	Configuration & Change Management	110 days	Tue 3/26/19	Wed 8/28/19
407	1.3.15.4	Testing	110 days	Tue 3/26/19	Wed 8/28/19
408	1.3.15.5	Network Connectivity & Configuration	110 days	Tue 3/26/19	Wed 8/28/19
409	1.3.15.6	PMS Support	110 days	Tue 3/26/19	Wed 8/28/19
410	1.3.15.7	System Security	110 days	Tue 3/26/19	Wed 8/28/19
411	**1.3.15.8**	**Technical Support Services**	**110 days**	**Tue 3/26/19**	**Wed 8/28/19**
412	1.3.15.8.1	Standup Tier 2/Tier 3 support	110 days	Tue 3/26/19	Wed 8/28/19

Page 4

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

ID	WBS	Task Name	Duration	Start	Finish
413	1.3.15.8.2	Provide PMS technical support	110 days	Tue 3/26/19	Wed 8/28/19
414	1.3.15.8.3	Coordinate resolution of escalated tickets and status tracking	110 days	Tue 3/26/19	Wed 8/28/19
415	**1.3.15.8.4**	**Trouble Ticket Reports**	**110 days**	**Tue 3/26/19**	**Wed 8/28/19**

Page 5

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

ID	WBS	Task Name	Duration	Start	Fini
325	**1.3.4.19**	**Sprint 8**	**10.5 days**	**Fri 1/18/19**	**Mo**
333	1.3.4.20	Milestone: Sprint 8 Complete	0 days	Fri 2/1/19	Fri 2
334	1.3.4.21	**Begin User Acceptance Testing (UAT)**	15 days	Mon 1/28/19	Fri 2
335	**1.3.4.22**	**Sprint 9**	**10.5 days**	**Tue 2/5/19**	**Tue**
343	1.3.4.23	Milestone: Sprint 9 Complete	0 days	Mon 2/18/19	Mo
344	**1.3.4.24**	**Perform Epic Business Review 3 with Stakeholders**	**2 days**	**Tue 2/19/19**	**We**
345	1.3.4.24.1	Provide User Stories from previous Sprints for End User usage	1 day	Tue 2/19/19	Tue
346	1.3.4.24.2	Provide simulated data for database and interfaces (as required)	1 day	Tue 2/19/19	Tue
347	1.3.4.24.3	Conduct Review of all User Stories and collect feedback	1 day	Wed 2/20/19	We
348					
349	**1.3.5**	**AHCCCS Milestone Gate Reviews**	**35 days**	**Tue 2/5/19**	**Mo**
350	1.3.5.1	Perform Penetration Test and provide results to AHCCCS and Med-QUEST	5 days	Tue 2/19/19	Mo
351	1.3.5.2	Develop Operational Readiness Review (ORR) Plan	5 days	Tue 2/5/19	Mo
352	1.3.5.3	Provide ORR Plan for AHCCCS/Med-QUEST Review and Approval	0 days	Mon 2/11/19	Mo
353	1.3.5.4	Prepare for ORR	10 days	Tue 2/12/19	Mo
354	1.3.5.5	Conduct Operational Readiness Review (ORR)	0 days	Mon 2/25/19	Mo
355	1.3.5.6	Prepare for PRR	10 days	Tue 2/26/19	Mo
356	1.3.5.7	Production Readiness Review (PRR) approval to Go Live	0 days	Mon 3/11/19	Mo
357	1.3.5.8	Prepare for Production Go Live	9 days	Tue 3/12/19	Fri 3
358	1.3.5.9	Go Live	0 days	Mon 3/25/19	Mo
359					
360	**1.3.6**	**HI Sprint 1**	**10 days**	**Wed 3/27/19**	**Tue**
368	1.3.7	Milestone: Sprint 1 Complete	0 days	Tue 4/9/19	Tue
369	**1.3.8**	**HI Sprint 2**	**10 days**	**Wed 4/10/19**	**Tue**
377	1.3.9	Milestone: Sprint 2 Complete	0 days	Tue 4/23/19	Tue
378	1.3.10	**Begin User Acceptance Testing (UAT)**	1 day?	Wed 4/17/19	We
379	**1.3.11**	**HI Sprint 3**	**10.5 days**	**Thu 4/25/19**	**Thu**
387	1.3.12	Milestone: Sprint 3 Complete	0 days	Thu 5/9/19	Thu
388	**1.3.13**	**Perform Epic Business Review 1 with Stakeholders**	**2 days**	**Thu 5/9/19**	**Mo**
389	1.3.13.1	Provide User Stories from previous Sprints for End User usage	1 day	Thu 5/9/19	Fri 5
390	1.3.13.2	Provide simulated data for database and interfaces (as required)	1 day	Thu 5/9/19	Fri 5
391	1.3.13.3	Conduct Review of all User Stories and collect feedback	1 day	Fri 5/10/19	Mo
392					
393	**1.3.14**	**HI Milestone Gate Reviews**	**26 days**	**Tue 4/23/19**	**Thu**
394	1.3.14.1	Develop Operational Readiness Review (ORR) Plan	6 days	Tue 4/23/19	We
395	1.3.14.2	Provide ORR Plan for AHCCCS/Med-QUEST Review and Approval	0 days	Wed 5/1/19	We
396	1.3.14.3	Prepare for ORR	5 days	Wed 5/1/19	We
397	1.3.14.4	Conduct Operational Readiness Review (ORR)	0 days	Wed 5/8/19	We
398	1.3.14.5	Prepare for PRR	5 days	Wed 5/8/19	We
399	1.3.14.6	Production Readiness Review approval to Go Live	0 days	Thu 5/16/19	Thu
400	1.3.14.7	Prepare for Production Go Live	10 days	Wed 5/15/19	Thu
401	1.3.14.8	Go Live	0 days	Thu 5/30/19	Thu
402					
403	**1.3.15**	**PMS Operations**	**110 days**	**Tue 3/26/19**	**We**
404	1.3.15.1	Project Management	110 days	Tue 3/26/19	We
405	1.3.15.2	Operations Monitoring & Reporting	110 days	Tue 3/26/19	We
406	1.3.15.3	Configuration & Change Management	110 days	Tue 3/26/19	We
407	1.3.15.4	Testing	110 days	Tue 3/26/19	We
408	1.3.15.5	Network Connectivity & Configuration	110 days	Tue 3/26/19	We
409	1.3.15.6	PMS Support	110 days	Tue 3/26/19	We
410	1.3.15.7	System Security	110 days	Tue 3/26/19	We
411	**1.3.15.8**	**Technical Support Services**	**110 days**	**Tue 3/26/19**	**We**
412	1.3.15.8.1	Standup Tier 2/Tier 3 support	110 days	Tue 3/26/19	We

Page 4

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

ID	WBS	Task Name	Duration	Start	Fini
325	**1.3.4.19**	**Sprint 8**	**10.5 days**	**Fri 1/18/19**	**Mo**
333	1.3.4.20	Milestone: Sprint 8 Complete	0 days	Fri 2/1/19	Fri 2
334	1.3.4.21	**Begin User Acceptance Testing (UAT)**	15 days	Mon 1/28/19	Fri 2
335	**1.3.4.22**	**Sprint 9**	**10.5 days**	**Tue 2/5/19**	**Tue**
343	1.3.4.23	Milestone: Sprint 9 Complete	0 days	Mon 2/18/19	Mo
344	**1.3.4.24**	**Perform Epic Business Review 3 with Stakeholders**	**2 days**	**Tue 2/19/19**	**We**
345	1.3.4.24.1	Provide User Stories from previous Sprints for End User usage	1 day	Tue 2/19/19	Tue
346	1.3.4.24.2	Provide simulated data for database and interfaces (as required)	1 day	Tue 2/19/19	Tue
347	1.3.4.24.3	Conduct Review of all User Stories and collect feedback	1 day	Wed 2/20/19	We
348					
349	**1.3.5**	**AHCCCS Milestone Gate Reviews**	**35 days**	**Tue 2/5/19**	**Mo**
350	1.3.5.1	Perform Penetration Test and provide results to AHCCCS and Med-QUEST	5 days	Tue 2/19/19	Mo
351	1.3.5.2	Develop Operational Readiness Review (ORR) Plan	5 days	Tue 2/5/19	Mo
352	1.3.5.3	Provide ORR Plan for AHCCCS/Med-QUEST Review and Approval	0 days	Mon 2/11/19	Mo
353	1.3.5.4	Prepare for ORR	10 days	Tue 2/12/19	Mo
354	1.3.5.5	Conduct Operational Readiness Review (ORR)	0 days	Mon 2/25/19	Mo
355	1.3.5.6	Prepare for PRR	10 days	Tue 2/26/19	Mo
356	1.3.5.7	Production Readiness Review (PRR) approval to Go Live	0 days	Mon 3/11/19	Mo
357	1.3.5.8	Prepare for Production Go Live	9 days	Tue 3/12/19	Fri 3
358	1.3.5.9	Go Live	0 days	Mon 3/25/19	Mo
359					
360	**1.3.6**	**HI Sprint 1**	**10 days**	**Wed 3/27/19**	**Tue**
368	1.3.7	Milestone: Sprint 1 Complete	0 days	Tue 4/9/19	Tue
369	**1.3.8**	**HI Sprint 2**	**10 days**	**Wed 4/10/19**	**Tue**
377	1.3.9	Milestone: Sprint 2 Complete	0 days	Tue 4/23/19	Tue
378	1.3.10	**Begin User Acceptance Testing (UAT)**	1 day?	Wed 4/17/19	We
379	**1.3.11**	**HI Sprint 3**	**10.5 days**	**Thu 4/25/19**	**Thu**
387	1.3.12	Milestone: Sprint 3 Complete	0 days	Thu 5/9/19	Thu
388	**1.3.13**	**Perform Epic Business Review 1 with Stakeholders**	**2 days**	**Thu 5/9/19**	**Mo**
389	1.3.13.1	Provide User Stories from previous Sprints for End User usage	1 day	Thu 5/9/19	Fri 5
390	1.3.13.2	Provide simulated data for database and interfaces (as required)	1 day	Thu 5/9/19	Fri 5
391	1.3.13.3	Conduct Review of all User Stories and collect feedback	1 day	Fri 5/10/19	Mo
392					
393	**1.3.14**	**HI Milestone Gate Reviews**	**26 days**	**Tue 4/23/19**	**Thu**
394	1.3.14.1	Develop Operational Readiness Review (ORR) Plan	6 days	Tue 4/23/19	We
395	1.3.14.2	Provide ORR Plan for AHCCCS/Med-QUEST Review and Approval	0 days	Wed 5/1/19	We
396	1.3.14.3	Prepare for ORR	5 days	Wed 5/1/19	We
397	1.3.14.4	Conduct Operational Readiness Review (ORR)	0 days	Wed 5/8/19	We
398	1.3.14.5	Prepare for PRR	5 days	Wed 5/8/19	We
399	1.3.14.6	Production Readiness Review approval to Go Live	0 days	Thu 5/16/19	Thu
400	1.3.14.7	Prepare for Production Go Live	10 days	Wed 5/15/19	Thu
401	1.3.14.8	Go Live	0 days	Thu 5/30/19	Thu
402					
403	**1.3.15**	**PMS Operations**	**110 days**	**Tue 3/26/19**	**We**
404	1.3.15.1	Project Management	110 days	Tue 3/26/19	We
405	1.3.15.2	Operations Monitoring & Reporting	110 days	Tue 3/26/19	We
406	1.3.15.3	Configuration & Change Management	110 days	Tue 3/26/19	We
407	1.3.15.4	Testing	110 days	Tue 3/26/19	We
408	1.3.15.5	Network Connectivity & Configuration	110 days	Tue 3/26/19	We
409	1.3.15.6	PMS Support	110 days	Tue 3/26/19	We
410	1.3.15.7	System Security	110 days	Tue 3/26/19	We
411	**1.3.15.8**	**Technical Support Services**	**110 days**	**Tue 3/26/19**	**We**
412	1.3.15.8.1	Standup Tier 2/Tier 3 support	110 days	Tue 3/26/19	We

Page 4

APPENDIX F: LIST OF ACRONYMS

Acronym/Abbreviation	Expansion/Definition
ACES	Automated Case Management and Eligibility System
ACID	Atomicity, Consistency, Isolation, Durability
ADA	Americans with Disabilities Act
ADE	Application Development Environment
ADOA	Arizona Department of Administration
AHCCCS	Arizona Health Care Cost Containment System
ANSI	American National Standards Institute

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

API	Application Programming Interface
APM	Application Performance Monitoring
ARS	Acceptable Risk Safeguards
ASET	Arizona Strategic Enterprise Technology
ATO	Authority to Operate
BAA	Business Associate Agreement
BI	Business Intelligence
BIRT	Business Intelligence and Reporting Tools; an open-source reporting technology with which Cúram integrates
BPEL	Business Process Execution Language
BPO	Business Process Object
BPR	Business Process Redesign
BPSSM	Business Partner System Security Manual
CADG	Cúram Analysis Documentation Generator
CAP	Corrective Action Plan
CARES	Client Assistance and Rehousing Enterprise System
CAS	Children Aid Societies
CCW	Chronic Condition Warehouse
CCW-VRDC	Chronic Condition Warehouse–Virtual Research Center
CDAT	Clinical Data Abstraction Tool
CEO	Chief Executive Officer
CER	Cúram Express Rules
CFACTS	CMS FISMA Control Tracking System
CHIP	Children's Health Insurance Program
CI/CD	Continuous Integration/Continuous Delivery
CISO	Chief Information Security Officer
CM	Configuration Management
CMMI	Capability Maturity Model Integration
CMS	Centers for Medicare and Medicaid
CON	Contract
COTS	Commercial Off-the-Shelf
CP	Contingency Plan
CPIN	Child Protection Information Network
CRD	Clinical Resource Directory
CPM	IBM Cúram Provider Management
CPU	Central Processing Unit
CSV	Comma Separated Values
CVO	Credentialing and Verification Organization
CYSSC	Children Youth and Social Services I&IT Cluster
Dev.	Development
DDI	Design, Development, and Implementation
DFDL	Data Format Description Language
DMP	Data Management Plan

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

DNS	Domain Name System
DOITT	Department of Information Technology and Telecommunications (New York City)
DOM	Document Object Model
DR	Disaster Recovery
DSG	Data and Systems Group
DUA	Data User Agreement
ECM	Enterprise Content Management
EDI	Electronic Data Interface
EIS	Eligibility Information Services
EPLS	Excluded Parties List System (now known as System for Award Management [SAM])
EPPE	Enterprise Privacy Policy Engine
ESB	Enterprise Service Bus
ESSO	Enterprise Single Sign-on
ETC	Estimate to Complete
EVM	Earned Value Management
FAQ	Frequently Asked Questions
FEA	Federal Enterprise Architecture
FHA	Federal Health Architecture
FIPS	Federal Information Processing Standard
FTI	File Type Information
FTP	File Transfer Protocol
HCC	Hierarchical Condition Category
HCR	Health Care Reform
HHS	U.S. Department of Health and Human Services
HHSC	Health and Human Services Commission
HIE	Health Information Exchange
HIPAA	Health Insurance Portability and Accountability Act
HIS	Hospital Information System
HITECH	Health Information Technology for Economic and Clinical Health (HITECH) Act
HL7	Health Level Seven International
HTML	Hypertext Markup Language
HTTPD	Hypertext Transfer Protocol Daemon (web server)
HTTPS	Hypertext Transfer Protocol Server
IaaS	Infrastructure as a Service
IAPD	Implementation Advance Planning Document
IBM	International Business Machines
IBM MQ	International Business Machines Message Queue
ID	Identification
IDS	Integrated Decision Support
IEG	Intelligent Evidence Gathering
IEPD	Information Exchange Package Documentation
IHSS	Integrated Human Services System (New York City)
IIB	IBM Integration Bus

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

IMS	Integrated Management System
Int	Integration
ISA	Interoperability Standards Advisory
ISO	International Standards Organization
ISP	Internet Service Provider
IT	Information Technology
ITIL	Information Technology Infrastructure Library
IV&V	Independent Verification and Validation
JAB	Joint Authorization Board
JAMIS	Joint Application Management Information System
JIRA	A truncation of Gojira, the Japanese name for Godzilla. Jira is a tool used for bug tracking, issue tracking, and project management, developed by Australian Company Atlassian.
JMS	Java Messaging Services
JSON	JavaScript Object Notation
JWT	Java Web Token
KMS	Knowledge Management System
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LEIE	List of Excluded Individual/Entities
LIS	Low Income Subsidy
MA	Medicare Advantage
MAO	Medicare Advantage Organization
MCBS	Medicare Current Beneficiary Survey
MACBIS	Medicaid and Children's Health Insurance Program Business Information Systems
MACBIS SI	Medicaid and Children's Health Insurance Program Business Information Systems System Integrator
MAG	Microsoft Azure for Government
MCO	Managed Care Organization
MCYS	Ministry of Children and Youth Services (Ontario)
MECL	Medicaid Enterprise Certification Life Cycle
MECT[1]	Medicaid Enterprise Certification Toolkit
MFA	Multi-factor Authentication
MITA	Medicaid Information Technology Architecture
MMIS	Medicaid Management Information System
MR	Medical Record
MS	Microsoft
NASA	National Aeronautics and Space Administration
NAT	National
NC FAST	North Carolina Families Accessing Services through Technology
NIEM	National Information Exchange Model
NIST	National Institute of Standards and Technology
NIST SP	National Institute of Standards and Technology Special Publication
NPI	National Provider Identifier

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

NPPES	National Plan and Provider Enrollment System
NSG	Network Security Group
NUCC	National Uniform Claim Committee
OACAS	Ontario's Association of Children's Aid Societies
OATH	Google Authenticator
OHA	Office of Hearings and Appeals
OOTB	Out-of-the-Box
ORR	Operational Readiness Review
OS	Operating System
PAPD	Planning Advance Planning Document
PCR	Priority, Complexity, and Risk
PDF	Portable Document Format
PECOS	Provider Enrollment, Chain and Ownership System (Medicare provider online enrollment system)
PHI	Protected Health Information
PI	Program Integrity
PII	Personally Identifiable Information
PMBOK	Project Management Book of Knowledge
PMI	Project Management Institute
PMO	Project Management Office
PMP	Project Management Plan
PMS	Provider Management System
PPQA	Process and Product Quality Assurance
PQPMI	Physician Quality Program Management Implementation
PRTG	Paessler Router Traffic Grapher
PSC	Provider Screening Challenge
PSTG	Private Sector Technology Group
PWP	Project Workplan
QA	Quality Assurance
QIO	Quality Improvement Organizations
QMO	Quality Management Office
RA	Remittance Advice
RACI	Responsible, Accountable, Consulted, and Informed
RADV CDAT	Risk Adjusted Data Validation Clinical Data Abstraction Tool
RAM	Responsibility Assignment Matrix
RASIC	Responsible, Approving, Supporting, Informed and Consulted—an employee uses these designations to define their relationship to parties for different parts of a project or corporation
RFP	Request for Proposal
RSA	IBM Rational Software Architect
RTM	Requirements Traceability Matrix
SAFe	Scalable Agile Framework
SAM	(IBM) Security Access Manager
SAML	Security Assertion Markup Language
SAS	Statistical Analysis System

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

SaaS	Software-as-a-Service
SCA	Security Controls Assessment
SCM	Software Configuration Management
SDD	Software Design Description
SDLC	Software Development Life Cycle
SIEM	Security Information and Event Management System
SIS	Single Information System
SLA	Service Level Agreement
SNAP	Supplemental Nutrition Assistance Program
SNMP	Simple Network Management Protocol
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SOW	Statement of Work
SPIP	Software Process Improvement Plan
SPM	Social Program Management
SPMP	Social Program Management Platform
SQL	Structured Query Language
SS-A	State Self-Assessment
SSI	Supplemental Security Income
SSL	Secure Sockets Layer
SSO	Single Sign-on
SSP	System Security Plan
SWIFT	Society For Worldwide Interbank Financial Telecommunications
TLS	Transport Layer Security
T-MSIS	Transformed Medicaid Statistical Information System
TRA	Technical Reference Architecture
TSR	Test Summary Reports
UAT	User Acceptance Testing
UDDI	Universal Description, Discovery, and Integration
UI/UX	User Interface/User Experience
UML	Uniform Modeling Language
USDS	United States Digital Services
Val	Validation
VHD	Virtual Hard Drives
VPN	Virtual Private Network
VRDC	Virtual Research Data Center
VSTS	Microsoft's Visual Studio Team System
W3C	World Wide Web Consortium
WAI	Web Accessibility Initiative
WAN/WLAN	Wide Area Network/Wireless Local Area Network
WBS	Work Breakdown Structures
WCAG	Web Content Accessibility Guidelines
WSDL	Web Service Description Language

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

XML	eXtensible Markup Language
X12	American National Standards Institute Accredited Standards Committee electronic data interchange standard

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

Add new demo site

Acronym/Abbreviation	Expansion/Definition
ACES	Automated Case Management and Eligibility System
ACID	Atomicity, Consistency, Isolation, Durability
ADA	Americans with Disabilities Act
ADE	Application Development Environment
ADOA	Arizona Department of Administration
AHCCCS	Arizona Health Care Cost Containment System
ANSI	American National Standards Institute
API	Application Programming Interface
APM	Application Performance Monitoring
ARS	Acceptable Risk Safeguards
ASET	Arizona Strategic Enterprise Technology
ATO	Authority to Operate
BAA	Business Associate Agreement
BI	Business Intelligence
BIRT	Business Intelligence and Reporting Tools; an open-source reporting technology with which Cúram integrates
BPEL	Business Process Execution Language
BPO	Business Process Object
BPR	Business Process Redesign
BPSSM	Business Partner System Security Manual
CADG	Cúram Analysis Documentation Generator
CAP	Corrective Action Plan
CARES	Client Assistance and Rehousing Enterprise System
CAS	Children Aid Societies
CCW	Chronic Condition Warehouse
CCW-VRDC	Chronic Condition Warehouse–Virtual Research Center
CDAT	Clinical Data Abstraction Tool
CEO	Chief Executive Officer
CER	Cúram Express Rules
CFACTS	CMS FISMA Control Tracking System
CHIP	Children's Health Insurance Program
CI/CD	Continuous Integration/Continuous Delivery
CISO	Chief Information Security Officer
CM	Configuration Management
CMMI	Capability Maturity Model Integration
CMS	Centers for Medicare and Medicaid
CON	Contract
COTS	Commercial Off-the-Shelf
CP	Contingency Plan

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

CPIN	Child Protection Information Network
CRD	Clinical Resource Directory
CPM	IBM Cúram Provider Management
CPU	Central Processing Unit
CSV	Comma Separated Values
CVO	Credentialing and Verification Organization
CYSSC	Children Youth and Social Services I&IT Cluster
Dev.	Development
DDI	Design, Development, and Implementation
DFDL	Data Format Description Language
DMP	Data Management Plan
DNS	Domain Name System
DOITT	Department of Information Technology and Telecommunications (New York City)
DOM	Document Object Model
DR	Disaster Recovery
DSG	Data and Systems Group
DUA	Data User Agreement
ECM	Enterprise Content Management
EDI	Electronic Data Interface
EIS	Eligibility Information Services
EPLS	Excluded Parties List System (now known as System for Award Management [SAM])
EPPE	Enterprise Privacy Policy Engine
ESB	Enterprise Service Bus
ESSO	Enterprise Single Sign-on
ETC	Estimate to Complete
EVM	Earned Value Management
FAQ	Frequently Asked Questions
FEA	Federal Enterprise Architecture
FHA	Federal Health Architecture
FIPS	Federal Information Processing Standard
FTI	File Type Information
FTP	File Transfer Protocol
HCC	Hierarchical Condition Category
HCR	Health Care Reform
HHS	U.S. Department of Health and Human Services
HHSC	Health and Human Services Commission
HIE	Health Information Exchange
HIPAA	Health Insurance Portability and Accountability Act
HIS	Hospital Information System
HITECH	Health Information Technology for Economic and Clinical Health (HITECH) Act
HL7	Health Level Seven International
HTML	Hypertext Markup Language
HTTPD	Hypertext Transfer Protocol Daemon (web server)

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

HTTPS	Hypertext Transfer Protocol Server
IaaS	Infrastructure as a Service
IAPD	Implementation Advance Planning Document
IBM	International Business Machines
IBM MQ	International Business Machines Message Queue
ID	Identification
IDS	Integrated Decision Support
IEG	Intelligent Evidence Gathering
IEPD	Information Exchange Package Documentation
IHSS	Integrated Human Services System (New York City)
IIB	IBM Integration Bus
IMS	Integrated Management System
Int	Integration
ISA	Interoperability Standards Advisory
ISO	International Standards Organization
ISP	Internet Service Provider
IT	Information Technology
ITIL	Information Technology Infrastructure Library
IV&V	Independent Verification and Validation
JAB	Joint Authorization Board
JAMIS	Joint Application Management Information System
JIRA	A truncation of Gojira, the Japanese name for Godzilla. Jira is a tool used for bug tracking, issue tracking, and project management, developed by Australian Company Atlassian.
JMS	Java Messaging Services
JSON	JavaScript Object Notation
JWT	Java Web Token
KMS	Knowledge Management System
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LEIE	List of Excluded Individual/Entities
LIS	Low Income Subsidy
MA	Medicare Advantage
MAO	Medicare Advantage Organization
MCBS	Medicare Current Beneficiary Survey
MACBIS	Medicaid and Children's Health Insurance Program Business Information Systems
MACBIS SI	Medicaid and Children's Health Insurance Program Business Information Systems System Integrator
MAG	Microsoft Azure for Government
MCO	Managed Care Organization
MCYS	Ministry of Children and Youth Services (Ontario)
MECL	Medicaid Enterprise Certification Life Cycle
MECT[1]	Medicaid Enterprise Certification Toolkit
MFA	Multi-factor Authentication

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

MITA	Medicaid Information Technology Architecture
MMIS	Medicaid Management Information System
MR	Medical Record
MS	Microsoft
NASA	National Aeronautics and Space Administration
NAT	National
NC FAST	North Carolina Families Accessing Services through Technology
NIEM	National Information Exchange Model
NIST	National Institute of Standards and Technology
NIST SP	National Institute of Standards and Technology Special Publication
NPI	National Provider Identifier
NPPES	National Plan and Provider Enrollment System
NSG	Network Security Group
NUCC	National Uniform Claim Committee
OACAS	Ontario's Association of Children's Aid Societies
OATH	Google Authenticator
OHA	Office of Hearings and Appeals
OOTB	Out-of-the-Box
ORR	Operational Readiness Review
OS	Operating System
PAPD	Planning Advance Planning Document
PCR	Priority, Complexity, and Risk
PDF	Portable Document Format
PECOS	Provider Enrollment, Chain and Ownership System (Medicare provider online enrollment system)
PHI	Protected Health Information
PI	Program Integrity
PII	Personally Identifiable Information
PMBOK	Project Management Book of Knowledge
PMI	Project Management Institute
PMO	Project Management Office
PMP	Project Management Plan
PMS	Provider Management System
PPQA	Process and Product Quality Assurance
PQPMI	Physician Quality Program Management Implementation
PRTG	Paessler Router Traffic Grapher
PSC	Provider Screening Challenge
PSTG	Private Sector Technology Group
PWP	Project Workplan
QA	Quality Assurance
QIO	Quality Improvement Organizations
QMO	Quality Management Office
RA	Remittance Advice
RACI	Responsible, Accountable, Consulted, and Informed

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

RADV CDAT	Risk Adjusted Data Validation Clinical Data Abstraction Tool
RAM	Responsibility Assignment Matrix
RASIC	Responsible, Approving, Supporting, Informed and Consulted—an employee uses these designations to define their relationship to parties for different parts of a project or corporation
RFP	Request for Proposal
RSA	IBM Rational Software Architect
RTM	Requirements Traceability Matrix
SAFe	Scalable Agile Framework
SAM	(IBM) Security Access Manager
SAML	Security Assertion Markup Language
SAS	Statistical Analysis System
SaaS	Software-as-a-Service
SCA	Security Controls Assessment
SCM	Software Configuration Management
SDD	Software Design Description
SDLC	Software Development Life Cycle
SIEM	Security Information and Event Management System
SIS	Single Information System
SLA	Service Level Agreement
SNAP	Supplemental Nutrition Assistance Program
SNMP	Simple Network Management Protocol
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SOW	Statement of Work
SPIP	Software Process Improvement Plan
SPM	Social Program Management
SPMP	Social Program Management Platform
SQL	Structured Query Language
SS-A	State Self-Assessment
SSI	Supplemental Security Income
SSL	Secure Sockets Layer
SSO	Single Sign-on
SSP	System Security Plan
SWIFT	Society For Worldwide Interbank Financial Telecommunications
TLS	Transport Layer Security
T-MSIS	Transformed Medicaid Statistical Information System
TRA	Technical Reference Architecture
TSR	Test Summary Reports
UAT	User Acceptance Testing
UDDI	Universal Description, Discovery, and Integration
UI/UX	User Interface/User Experience
UML	Uniform Modeling Language
USDS	United States Digital Services

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

Val	Validation
VHD	Virtual Hard Drives
VPN	Virtual Private Network
VRDC	Virtual Research Data Center
VSTS	Microsoft's Visual Studio Team System
W3C	World Wide Web Consortium
WAI	Web Accessibility Initiative
WAN/WLAN	Wide Area Network/Wireless Local Area Network
WBS	Work Breakdown Structures
WCAG	Web Content Accessibility Guidelines
WSDL	Web Service Description Language
XML	eXtensible Markup Language
X12	American National Standards Institute Accredited Standards Committee electronic data interchange standard

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

Acronym/Abbreviation	Expansion/Definition
ACES	Automated Case Management and Eligibility System
ACID	Atomicity, Consistency, Isolation, Durability
ADA	Americans with Disabilities Act
ADE	Application Development Environment
ADOA	Arizona Department of Administration
AHCCCS	Arizona Health Care Cost Containment System
ANSI	American National Standards Institute
API	Application Programming Interface
APM	Application Performance Monitoring
ARS	Acceptable Risk Safeguards
ASET	Arizona Strategic Enterprise Technology
ATO	Authority to Operate
BAA	Business Associate Agreement
BI	Business Intelligence
BIRT	Business Intelligence and Reporting Tools; an open-source reporting technology with which Cúram integrates
BPEL	Business Process Execution Language
BPO	Business Process Object
BPR	Business Process Redesign
BPSSM	Business Partner System Security Manual
CADG	Cúram Analysis Documentation Generator
CAP	Corrective Action Plan
CARES	Client Assistance and Rehousing Enterprise System
CAS	Children Aid Societies
CCW	Chronic Condition Warehouse
CCW-VRDC	Chronic Condition Warehouse–Virtual Research Center
CDAT	Clinical Data Abstraction Tool
CEO	Chief Executive Officer
CER	Cúram Express Rules
CFACTS	CMS FISMA Control Tracking System
CHIP	Children's Health Insurance Program
CI/CD	Continuous Integration/Continuous Delivery
CISO	Chief Information Security Officer
CM	Configuration Management
CMMI	Capability Maturity Model Integration
CMS	Centers for Medicare and Medicaid
CON	Contract
COTS	Commercial Off-the-Shelf
CP	Contingency Plan
CPIN	Child Protection Information Network
CRD	Clinical Resource Directory
CPM	IBM Cúram Provider Management

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

CPU	Central Processing Unit
CSV	Comma Separated Values
CVO	Credentialing and Verification Organization
CYSSC	Children Youth and Social Services I&IT Cluster
Dev.	Development
DDI	Design, Development, and Implementation
DFDL	Data Format Description Language
DMP	Data Management Plan
DNS	Domain Name System
DOITT	Department of Information Technology and Telecommunications (New York City)
DOM	Document Object Model
DR	Disaster Recovery
DSG	Data and Systems Group
DUA	Data User Agreement
ECM	Enterprise Content Management
EDI	Electronic Data Interface
EIS	Eligibility Information Services
EPLS	Excluded Parties List System (now known as System for Award Management [SAM])
EPPE	Enterprise Privacy Policy Engine
ESB	Enterprise Service Bus
ESSO	Enterprise Single Sign-on
ETC	Estimate to Complete
EVM	Earned Value Management
FAQ	Frequently Asked Questions
FEA	Federal Enterprise Architecture
FHA	Federal Health Architecture
FIPS	Federal Information Processing Standard
FTI	File Type Information
FTP	File Transfer Protocol
HCC	Hierarchical Condition Category
HCR	Health Care Reform
HHS	U.S. Department of Health and Human Services
HHSC	Health and Human Services Commission
HIE	Health Information Exchange
HIPAA	Health Insurance Portability and Accountability Act
HIS	Hospital Information System
HITECH	Health Information Technology for Economic and Clinical Health (HITECH) Act
HL7	Health Level Seven International
HTML	Hypertext Markup Language
HTTPD	Hypertext Transfer Protocol Daemon (web server)
HTTPS	Hypertext Transfer Protocol Server
IaaS	Infrastructure as a Service
IAPD	Implementation Advance Planning Document

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

IBM	International Business Machines
IBM MQ	International Business Machines Message Queue
ID	Identification
IDS	Integrated Decision Support
IEG	Intelligent Evidence Gathering
IEPD	Information Exchange Package Documentation
IHSS	Integrated Human Services System (New York City)
IIB	IBM Integration Bus
IMS	Integrated Management System
Int	Integration
ISA	Interoperability Standards Advisory
ISO	International Standards Organization
ISP	Internet Service Provider
IT	Information Technology
ITIL	Information Technology Infrastructure Library
IV&V	Independent Verification and Validation
JAB	Joint Authorization Board
JAMIS	Joint Application Management Information System
JIRA	A truncation of Gojira, the Japanese name for Godzilla. Jira is a tool used for bug tracking, issue tracking, and project management, developed by Australian Company Atlassian.
JMS	Java Messaging Services
JSON	JavaScript Object Notation
JWT	Java Web Token
KMS	Knowledge Management System
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LEIE	List of Excluded Individual/Entities
LIS	Low Income Subsidy
MA	Medicare Advantage
MAO	Medicare Advantage Organization
MCBS	Medicare Current Beneficiary Survey
MACBIS	Medicaid and Children's Health Insurance Program Business Information Systems
MACBIS SI	Medicaid and Children's Health Insurance Program Business Information Systems System Integrator
MAG	Microsoft Azure for Government
MCO	Managed Care Organization
MCYS	Ministry of Children and Youth Services (Ontario)
MECL	Medicaid Enterprise Certification Life Cycle
MECT[1]	Medicaid Enterprise Certification Toolkit
MFA	Multi-factor Authentication
MITA	Medicaid Information Technology Architecture
MMIS	Medicaid Management Information System
MR	Medical Record

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

MS	Microsoft
NASA	National Aeronautics and Space Administration
NAT	National
NC FAST	North Carolina Families Accessing Services through Technology
NIEM	National Information Exchange Model
NIST	National Institute of Standards and Technology
NIST SP	National Institute of Standards and Technology Special Publication
NPI	National Provider Identifier
NPPES	National Plan and Provider Enrollment System
NSG	Network Security Group
NUCC	National Uniform Claim Committee
OACAS	Ontario's Association of Children's Aid Societies
OATH	Google Authenticator
OHA	Office of Hearings and Appeals
OOTB	Out-of-the-Box
ORR	Operational Readiness Review
OS	Operating System
PAPD	Planning Advance Planning Document
PCR	Priority, Complexity, and Risk
PDF	Portable Document Format
PECOS	Provider Enrollment, Chain and Ownership System (Medicare provider online enrollment system)
PHI	Protected Health Information
PI	Program Integrity
PII	Personally Identifiable Information
PMBOK	Project Management Book of Knowledge
PMI	Project Management Institute
PMO	Project Management Office
PMP	Project Management Plan
PMS	Provider Management System
PPQA	Process and Product Quality Assurance
PQPMI	Physician Quality Program Management Implementation
PRTG	Paessler Router Traffic Grapher
PSC	Provider Screening Challenge
PSTG	Private Sector Technology Group
PWP	Project Workplan
QA	Quality Assurance
QIO	Quality Improvement Organizations
QMO	Quality Management Office
RA	Remittance Advice
RACI	Responsible, Accountable, Consulted, and Informed
RADV CDAT	Risk Adjusted Data Validation Clinical Data Abstraction Tool
RAM	Responsibility Assignment Matrix
RASIC	Responsible, Approving, Supporting, Informed and Consulted—an employee uses these

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

	designations to define their relationship to parties for different parts of a project or corporation
RFP	Request for Proposal
RSA	IBM Rational Software Architect
RTM	Requirements Traceability Matrix
SAFe	Scalable Agile Framework
SAM	(IBM) Security Access Manager
SAML	Security Assertion Markup Language
SAS	Statistical Analysis System
SaaS	Software-as-a-Service
SCA	Security Controls Assessment
SCM	Software Configuration Management
SDD	Software Design Description
SDLC	Software Development Life Cycle
SIEM	Security Information and Event Management System
SIS	Single Information System
SLA	Service Level Agreement
SNAP	Supplemental Nutrition Assistance Program
SNMP	Simple Network Management Protocol
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SOW	Statement of Work
SPIP	Software Process Improvement Plan
SPM	Social Program Management
SPMP	Social Program Management Platform
SQL	Structured Query Language
SS-A	State Self-Assessment
SSI	Supplemental Security Income
SSL	Secure Sockets Layer
SSO	Single Sign-on
SSP	System Security Plan
SWIFT	Society For Worldwide Interbank Financial Telecommunications
TLS	Transport Layer Security
T-MSIS	Transformed Medicaid Statistical Information System
TRA	Technical Reference Architecture
TSR	Test Summary Reports
UAT	User Acceptance Testing
UDDI	Universal Description, Discovery, and Integration
UI/UX	User Interface/User Experience
UML	Uniform Modeling Language
USDS	United States Digital Services
Val	Validation
VHD	Virtual Hard Drives
VPN	Virtual Private Network

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

VRDC	Virtual Research Data Center
VSTS	Microsoft's Visual Studio Team System
W3C	World Wide Web Consortium
WAI	Web Accessibility Initiative
WAN/WLAN	Wide Area Network/Wireless Local Area Network
WBS	Work Breakdown Structures
WCAG	Web Content Accessibility Guidelines
WSDL	Web Service Description Language
XML	eXtensible Markup Language
X12	American National Standards Institute Accredited Standards Committee electronic data interchange standard

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

Acronym/Abbreviation	Expansion/Definition
ACES	Automated Case Management and Eligibility System
ACID	Atomicity, Consistency, Isolation, Durability
ADA	Americans with Disabilities Act
ADE	Application Development Environment
ADOA	Arizona Department of Administration
AHCCCS	Arizona Health Care Cost Containment System
ANSI	American National Standards Institute
API	Application Programming Interface
APM	Application Performance Monitoring
ARS	Acceptable Risk Safeguards
ASET	Arizona Strategic Enterprise Technology
ATO	Authority to Operate
BAA	Business Associate Agreement
BI	Business Intelligence
BIRT	Business Intelligence and Reporting Tools; an open-source reporting technology with which Cúram integrates
BPEL	Business Process Execution Language
BPO	Business Process Object
BPR	Business Process Redesign
BPSSM	Business Partner System Security Manual
CADG	Cúram Analysis Documentation Generator
CAP	Corrective Action Plan
CARES	Client Assistance and Rehousing Enterprise System
CAS	Children Aid Societies
CCW	Chronic Condition Warehouse
CCW-VRDC	Chronic Condition Warehouse–Virtual Research Center
CDAT	Clinical Data Abstraction Tool
CEO	Chief Executive Officer
CER	Cúram Express Rules
CFACTS	CMS FISMA Control Tracking System
CHIP	Children's Health Insurance Program
CI/CD	Continuous Integration/Continuous Delivery
CISO	Chief Information Security Officer
CM	Configuration Management
CMMI	Capability Maturity Model Integration
CMS	Centers for Medicare and Medicaid
CON	Contract
COTS	Commercial Off-the-Shelf
CP	Contingency Plan
CPIN	Child Protection Information Network
CRD	Clinical Resource Directory
CPM	IBM Cúram Provider Management

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

CPU	Central Processing Unit
CSV	Comma Separated Values
CVO	Credentialing and Verification Organization
CYSSC	Children Youth and Social Services I&IT Cluster
Dev.	Development
DDI	Design, Development, and Implementation
DFDL	Data Format Description Language
DMP	Data Management Plan
DNS	Domain Name System
DOITT	Department of Information Technology and Telecommunications (New York City)
DOM	Document Object Model
DR	Disaster Recovery
DSG	Data and Systems Group
DUA	Data User Agreement
ECM	Enterprise Content Management
EDI	Electronic Data Interface
EIS	Eligibility Information Services
EPLS	Excluded Parties List System (now known as System for Award Management [SAM])
EPPE	Enterprise Privacy Policy Engine
ESB	Enterprise Service Bus
ESSO	Enterprise Single Sign-on
ETC	Estimate to Complete
EVM	Earned Value Management
FAQ	Frequently Asked Questions
FEA	Federal Enterprise Architecture
FHA	Federal Health Architecture
FIPS	Federal Information Processing Standard
FTI	File Type Information
FTP	File Transfer Protocol
HCC	Hierarchical Condition Category
HCR	Health Care Reform
HHS	U.S. Department of Health and Human Services
HHSC	Health and Human Services Commission
HIE	Health Information Exchange
HIPAA	Health Insurance Portability and Accountability Act
HIS	Hospital Information System
HITECH	Health Information Technology for Economic and Clinical Health (HITECH) Act
HL7	Health Level Seven International
HTML	Hypertext Markup Language
HTTPD	Hypertext Transfer Protocol Daemon (web server)
HTTPS	Hypertext Transfer Protocol Server
IaaS	Infrastructure as a Service
IAPD	Implementation Advance Planning Document

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

IBM	International Business Machines
IBM MQ	International Business Machines Message Queue
ID	Identification
IDS	Integrated Decision Support
IEG	Intelligent Evidence Gathering
IEPD	Information Exchange Package Documentation
IHSS	Integrated Human Services System (New York City)
IIB	IBM Integration Bus
IMS	Integrated Management System
Int	Integration
ISA	Interoperability Standards Advisory
ISO	International Standards Organization
ISP	Internet Service Provider
IT	Information Technology
ITIL	Information Technology Infrastructure Library
IV&V	Independent Verification and Validation
JAB	Joint Authorization Board
JAMIS	Joint Application Management Information System
JIRA	A truncation of Gojira, the Japanese name for Godzilla. Jira is a tool used for bug tracking, issue tracking, and project management, developed by Australian Company Atlassian.
JMS	Java Messaging Services
JSON	JavaScript Object Notation
JWT	Java Web Token
KMS	Knowledge Management System
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LEIE	List of Excluded Individual/Entities
LIS	Low Income Subsidy
MA	Medicare Advantage
MAO	Medicare Advantage Organization
MCBS	Medicare Current Beneficiary Survey
MACBIS	Medicaid and Children's Health Insurance Program Business Information Systems
MACBIS SI	Medicaid and Children's Health Insurance Program Business Information Systems System Integrator
MAG	Microsoft Azure for Government
MCO	Managed Care Organization
MCYS	Ministry of Children and Youth Services (Ontario)
MECL	Medicaid Enterprise Certification Life Cycle
MECT[1]	Medicaid Enterprise Certification Toolkit
MFA	Multi-factor Authentication
MITA	Medicaid Information Technology Architecture
MMIS	Medicaid Management Information System
MR	Medical Record

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

MS	Microsoft
NASA	National Aeronautics and Space Administration
NAT	National
NC FAST	North Carolina Families Accessing Services through Technology
NIEM	National Information Exchange Model
NIST	National Institute of Standards and Technology
NIST SP	National Institute of Standards and Technology Special Publication
NPI	National Provider Identifier
NPPES	National Plan and Provider Enrollment System
NSG	Network Security Group
NUCC	National Uniform Claim Committee
OACAS	Ontario's Association of Children's Aid Societies
OATH	Google Authenticator
OHA	Office of Hearings and Appeals
OOTB	Out-of-the-Box
ORR	Operational Readiness Review
OS	Operating System
PAPD	Planning Advance Planning Document
PCR	Priority, Complexity, and Risk
PDF	Portable Document Format
PECOS	Provider Enrollment, Chain and Ownership System (Medicare provider online enrollment system)
PHI	Protected Health Information
PI	Program Integrity
PII	Personally Identifiable Information
PMBOK	Project Management Book of Knowledge
PMI	Project Management Institute
PMO	Project Management Office
PMP	Project Management Plan
PMS	Provider Management System
PPQA	Process and Product Quality Assurance
PQPMI	Physician Quality Program Management Implementation
PRTG	Paessler Router Traffic Grapher
PSC	Provider Screening Challenge
PSTG	Private Sector Technology Group
PWP	Project Workplan
QA	Quality Assurance
QIO	Quality Improvement Organizations
QMO	Quality Management Office
RA	Remittance Advice
RACI	Responsible, Accountable, Consulted, and Informed
RADV CDAT	Risk Adjusted Data Validation Clinical Data Abstraction Tool
RAM	Responsibility Assignment Matrix
RASIC	Responsible, Approving, Supporting, Informed and Consulted—an employee uses these

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

	designations to define their relationship to parties for different parts of a project or corporation
RFP	Request for Proposal
RSA	IBM Rational Software Architect
RTM	Requirements Traceability Matrix
SAFe	Scalable Agile Framework
SAM	(IBM) Security Access Manager
SAML	Security Assertion Markup Language
SAS	Statistical Analysis System
SaaS	Software-as-a-Service
SCA	Security Controls Assessment
SCM	Software Configuration Management
SDD	Software Design Description
SDLC	Software Development Life Cycle
SIEM	Security Information and Event Management System
SIS	Single Information System
SLA	Service Level Agreement
SNAP	Supplemental Nutrition Assistance Program
SNMP	Simple Network Management Protocol
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SOW	Statement of Work
SPIP	Software Process Improvement Plan
SPM	Social Program Management
SPMP	Social Program Management Platform
SQL	Structured Query Language
SS-A	State Self-Assessment
SSI	Supplemental Security Income
SSL	Secure Sockets Layer
SSO	Single Sign-on
SSP	System Security Plan
SWIFT	Society For Worldwide Interbank Financial Telecommunications
TLS	Transport Layer Security
T-MSIS	Transformed Medicaid Statistical Information System
TRA	Technical Reference Architecture
TSR	Test Summary Reports
UAT	User Acceptance Testing
UDDI	Universal Description, Discovery, and Integration
UI/UX	User Interface/User Experience
UML	Uniform Modeling Language
USDS	United States Digital Services
Val	Validation
VHD	Virtual Hard Drives
VPN	Virtual Private Network

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.

VRDC	Virtual Research Data Center
VSTS	Microsoft's Visual Studio Team System
W3C	World Wide Web Consortium
WAI	Web Accessibility Initiative
WAN/WLAN	Wide Area Network/Wireless Local Area Network
WBS	Work Breakdown Structures
WCAG	Web Content Accessibility Guidelines
WSDL	Web Service Description Language
XML	eXtensible Markup Language
X12	American National Standards Institute Accredited Standards Committee electronic data interchange standard

Use or disclosure of data contained on this page is subject to the restriction on the cover sheet of this proposal or quotation.