Table of Contents

9.7 Control and Security Requirement 1
Meeting HIPAA Controls and Security Standards 1
Physical and Logical Security 2
HIPAA Security Compliance 3
Implementation and Maintenance for Security Infrastructure 3
Planned Maintenance and Updates 3
HMS Ensures the Integrity of Our System and Client Data 4
Methods and Controls 4
HMS Staff Are Trained to Protect Our Clients' Data 5
Procedures for Data Storage, Management, and Back-up 5
Destruction of Protected Data 6
Protecting PHI 7
Active Data (Transmission) 7
Encryption 7
File Exchange 8
Data at Rest (Stored) 8
Offsite Data Storage 9
Release of Information 9
Monitoring Suspect Activity 9
Restricting Access to Facilities 10
Audit Controls to Monitor Physical and System Access 10
Tracking and Documenting Security Updates 11

This page intentionally left blank.

9.7 Control and Security Requirement

RFP Reference: 11.

HMS has strong, long-standing processes for physical and logical security that ensure that we safeguard AHCCCS's records and maintain those records in accordance with both state and federal laws and regulations, such as HIPAA and Health Information Technology for Economic and Clinical Health (HITECH) data security laws and regulations. Our processes have been proven effective for more than 30 years and not only meet but also exceed requirements pertaining to the 42 specific administrative procedures identified in HIPAA security rules, which detail provisions regarding physical safeguards and logical/technical security processes put in place to guard the Confidentiality, Integrity, and Availability (CIA) of electronic PHI (ePHI).

HMS achieved its first certification under the HITRUST Common Security Framework (CSF) in 2014 and were recently recertified through 2019. HITRUST has established the CSF, a certifiable information security framework that can be used by organizations that create, access, store or exchange personal health or financial information. HMS adopted the CSF to demonstrate our commitment to the protection and security of ePHI.

The following pages detail our ability to maintain information security.

Meeting HIPAA Controls and Security Standards

RFP Reference: 11.

> The Contractor shall provide adequate controls and security in accordance with HIPAA standards as approved by AHCCCS to maintain the integrity and confidentiality of computerized data. In addition, the Contractor shall provide documentation of its data control and security systems to enable AHCCCS to evaluate the adequacy of such systems, as evidenced by an annual audit (SSAE 16) by an outside firm, approved in advance by AHCCCS, of the security of its systems and stored data.

HMS recognizes that management of risk is a crucial part of the service that we deliver to our clients. Our methodology not only appropriately identifies and validates improper payments and communicates findings clearly to providers, but also safeguards the data entrusted to us. To this end, we invest more than $50 million each year in IT and in ensuring the security of the systems, infrastructure, and technology that we have in place throughout the country. HMS will continue to invest in the resources required to manage our clients' data in a manner that is not only secure but also in full compliance with state and federal rules and regulations.

HMS's data security measures are the result of proven, tested methodologies designed to not only safeguard the government and public health clients who entrust us to ensure the integrity of their data but also protect the vulnerability of the citizens whom each program serves. The pillars of CIA—Confidentiality, Integrity, and Availability—are the primary security objectives cited in federal regulations regarding IT security. These objectives describe the paramount goals for ensuring the protection of information and resources from unauthorized access, use, disclosure, disruption, modification, or destruction, as follows:

- **Confidentiality**—preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. The assigned level of confidentiality

is used in determining the types of security measures required for its protection from unauthorized access or disclosure.

- **Integrity**—guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity. The level of impact of the unauthorized modification or destruction of information resources determines the importance of maintaining the integrity of a resource.
- **Availability**—ensuring timely and reliable access to and use of information. The overall importance of the availability of a resource is based on its criticality to the functional operation of the Department or the priority placed on said function in continuity plans and disaster recovery strategies. Emergency management planning must take into account the availability requirements of a particular resource to determine its inclusion in emergency and disaster recovery planning.

Physical and Logical Security

HMS provides an Enterprise Security Architecture (ESA) that underlies our strategic plan for maintaining physical and logical security across the HMS organization, ensuring that our processes align with all internal and external security requirements. This architecture details five key components of information security architecture and provides step-by-step guidance on how to analyze, develop, and implement a logical and effective program that achieves the security objectives.

The key components of our information security architecture are:

- Organization and Infrastructure
- Policies and Procedures
- Security Baselines of Systems Components
- Security Awareness and Training
- Compliance

The security objectives of the ESA are derived from HMS business requirements in addition to all applicable regulatory requirements (i.e., NIST, FISMA, HIPAA). HMS deploys the ESA across our organization at the process, technology, and person level to ensure the consistency and redundancy of our security measures. The following Capability Curves are key elements within the HMS ESA design:

- Security Organization
- Regulatory Compliance
- Policy Management
- Security Awareness
- Measurement and Reporting
- IT and Asset Management
- Incident Management
- Threat and Vulnerability Management

- Identity Management
- Business Continuity Planning

We are confident that our physical and logical standards, which meet the standards required for states and the federal government, including CMS, meet or exceed AHCCCS's requirements.

HIPAA Security Compliance

As part of HMS's Corporate Compliance program, HMS maintains our services to meet the standards mandated by the HIPAA Privacy Rule. Our HIPAA security compliance methodology goes beyond the requirements of the HIPAA Security Rule; it serves as a road map to safeguard not just ePHI but HMS information assets as a whole. This methodology has been influenced by the domains defined in the International Organization for Standardization (ISO) standard ISO 17799, the British Standards (BS) BS 7799 security standards, and the Control Objectives for Information and Related Technology (CobIT) security frameworks.

Implementation and Maintenance for Security Infrastructure

HMS maintains a secure processing environment. Through annual and as-necessary reviews of our policies and procedures and exercises designed to test our secure environment, we continually build our system for security. It is HMS's policy that we handle all data according to strict protocols, document and maintain that information in a central database, and update it as necessary. Likewise, all data handling protocols address data security in accordance with both state and federal requirements and are specifically written to each client's unique specifications, including AHCCCS's. Where necessary, HMS modifies our approach to meet or exceed all applicable state and federal statutes concerning data security and confidentiality, including any client-specific requirements pertaining to data security in general and to patient/clinical data in particular.

Furthermore, HMS continually ensures that our contract work complies with the standards concerning transfer of data, data confidentiality, and other requirements identified in HIPAA. To ensure that we remain in compliance, HMS established a Security Review committee, which is a team comprised of HMS compliance experts who review and audit our compliance with security and HIPAA policies and procedures. Chaired by HMS's Chief Compliance Officer (CCO) and Chief Security Officer (CSO), this committee includes senior technical managers and representatives from each business area.

Planned Maintenance and Updates

HMS's CSO maintains our Data Security plan as well as our Facility Security plan containing procedures to safeguard all facilities, systems, and equipment used to store PHI against unauthorized physical access, tampering, or theft. The CSO will review the plans every six months and incorporate any necessary updates regarding contingency operations, access control and validation, physical access records, and maintenance.

Since our inception more than 30 years ago, HMS's focus has been on designing, fine-tuning, and evolving the security of our corporate infrastructure to meet ever-changing business needs. We

acknowledge that information and information systems are vitally important HMS business assets. We further understand that without reliable and properly secured information and information systems, HMS would face significant risks to the viability and continued success of our business. Likewise, the preservation and enhancement of our reputation depends in part on the way in which we manage both information and information systems. Laws such as HIPAA, the Sarbanes-Oxley (SOX) Act, and American Recovery and Reinvestment Act of 2009 (ARRA) serve as guidelines for our data security processes and procedures.

HMS Ensures the Integrity of Our System and Client Data

As an industry leader in the healthcare information services field, HMS recognizes our clients' need for the highest level of data/system integrity and security. To ensure that our clients' data is never compromised, we offer a multilevel security system that fully protects against physical damage and prevents unauthorized access to data and systems. In addition, to meet the demanding standards and considerable sensitivities of local, state, and federal entities, HMS developed sophisticated measures to guarantee confidentiality. We protect the confidentiality of all personal, financial, clinical, and employment information pertaining to our clients and the individuals whom each program serves.

HMS Security and Internal Audit teams regularly perform internal audits of system controls and security, including an annual Statement on Standards for Attestation Engagements (SSAE) 16 audit. As the TPL scope of work requires, HMS will annually submit an SSAE 16 SOC 1 Report during the contract term.

Methods and Controls

We ensure the security of our systems and data by implementing methods designed to prevent and minimize potential damage and interruption that may make data or applications containing warehouse data unavailable. HMS realizes that locally developed applications may become critical to the mission of campus units, and we have developed controls to provide service continuity based on the criticality of the data or the unit's application to the mission. Our methods include:

- Appropriately trained staff. Management has taken the steps necessary to ensure adequate staffing for data and applications that we consider critical to the functioning of the unit.
- Back-up of data and applications. We securely back up or replicate data files onto encrypted storage devices. Back-up schemes used include nightly or weekly dual tape back-ups, storing one copy remotely. For applications with many transactions, we may consider transaction logging in addition to tape or replication copies. HMS has an effective back-up process that allows recovery of all data and applications with minimal time and effort.
- Protocols for protecting client data. HMS has multilayer procedures and protocols in place related to protecting our clients' data, including measures for securing active and stored data and monitoring access to data and facilities. We are committed to maintaining our reputation as a trustworthy partner to our clients.

HMS Staff Are Trained to Protect Our Clients' Data

HMS's CSO holds responsibility for the initial and ongoing training of the workforce. HMS understands the importance of training staff to ensure system and data integrity and compliance with state and federal regulations as well as our clients' requirements. Our corporate risk management training emphasizes the importance of security and compliance issues to employees throughout their tenure at the company—beginning with initial employee orientation and training. Upon accepting employment, all employees are required to:

- Affirm that they have read the Corporate Compliance Handbook (including the formal policies and Corporate Compliance Statement that it contains)
- Undergo initial Corporate Compliance program and HIPAA Privacy training
- Attest to understanding the statement and policies and will abide by and conform to the rules set forth within them

On an annual basis, staff undergo a thorough training session that not only details all components of the Data Security plan but also advises HMS staff of any recently implemented plan modifications. Our Security team reinforces this training through a monthly security awareness newsletter. Each team member must attend this training on an annual basis, at a minimum, to ensure that all key members of the team are kept abreast of plan specifications. We test employee understanding of policies at the time of training, and throughout the year, supervisors manage employee adherence to HMS policies and further assess compliance through annual performance evaluations.

Procedures for Data Storage, Management, and Back-up

HMS follows detailed data management procedures that address the data files and tapes that clients entrust to us as well as the work product associated with HMS's ongoing performance of contracted tasks.

When HMS receives a client data file/tape (or creates a file), we identify the data and associated client and determine:

- How HMS will use the data
- Which HMS employee(s) will have access rights to the data
- Which HMS employee(s) will need to know if there are problems with the data
- When and how to return client data

HMS creates a unique Data Identification Protocol to track all data and its specific characteristics. This management system enables HMS to handle large volumes of data securely—with constant control of all input and output. When we first receive client data, either electronically or in another format, the data is external to HMS's secure processing environment. To ensure security, HMS copies data to the current addressed storage library, where we can manage, control, and audit it.

HMS currently stores all physical data back-ups offsite with Iron Mountain, the country's premier, secure data storage company. If a file must be restored, HMS can access the tapes within two hours and begin

the restoration process. To provide additional protection, we encrypt all back-up volumes that we send offsite.

To ensure that we maintain important client- and company-specific information, we back up all data storage and Local Area Network (LAN) file server devices using full-volume back-ups and real-time replication procedures, as may be dictated.

We perform the following types of back-ups:

- Physical back-ups. For all physical back-ups, HMS maintains a rotation process via the logging and tracking policy. We conduct two types of physical back-ups:
  - Daily incremental back-ups, which include any changes to our system and control files
  - Weekly full-system back-ups, which include programs, operating systems, and control files
- Replication. For real-time replication, the replication process begins at the point at which HMS internalizes the data. We replicate all data that is labeled “Source Data” to HMS-dedicated storage devices in our disaster recovery hot site, which is located in an HMS secure hosting cage.

Destruction of Protected Data

In accordance with ARRA guidelines, it is HMS’s policy to destroy all physical media containing PHI unless we are required to retain original documentation by client instruction or contract requirements. We dispose of media containing PHI daily and do so in a manner that protects that PHI from being used or disclosed in any way. We ensure that such information is destroyed beyond capacity to read it, and we shred all paper media. Also, as part of our documented Training program, HMS educates every employee on the importance of destroying all paperwork prior to leaving the office each day as well as storing any paperwork in process in a secure, locked environment during nonbusiness hours.

We adhere to the following protocols:

- Prior to destroying or disposing of any storage device or removal medium, we ensure that the device or medium does not contain PHI.
- Use of data destruction tools in instances where a typical reformat is not sufficient because it does not overwrite the data. For example, if the device or medium contained PHI that is no longer required or needed and is not a unique copy, we must use a data destruction tool prior to disposal to ensure the complete destruction of the data/information.
- Electronic documents. We send all storage media, such as computer hard drives, flash drives, CD/DVDs, and tape containing AHCCCS-protected or sensitive data in electronic form to the ITS Director of Operations for secure deletion. The ITS Director, under guidance of the Security Information Officer, will delete AHCCCS-protected or sensitive data from the media in accordance with current ARRA guidelines. An HMS-contracted service will destroy, by smashing or degaussing, any media that cannot be processed according to this standard.
- Paper documents. All Arizona-protected and sensitive data existing in paper form must be disposed of by shredding. All documents will be dropped off in designated containers, and the contents will be shredded by a licensed and bonded document destruction company.

PROTECTING PHI

It is HMS policy to employ a variety of security measures to ensure the confidentiality of sensitive healthcare information, including methods to encrypt, store, and transport data; to protect information while actively in use or at rest; and to adhere to Code of Federal Regulations (CFR) 45 CFR Parts 160, 162, and 164.

ACTIVE DATA (TRANSMISSION)

For HMS, the secure transmission of AHCCCS's data is a primary focus to ensure that PHI is protected appropriately and that data exchanges are accomplished in accordance with AHCCCS's guidelines. HMS has a long history of maintaining the privacy of this type of information and has extensive experience in the secure handling of client information.

HMS deploys numerous secure connections to all clients via 3DES or 256 AES VPN tunneling technology for secure transfers of data. For physical media transfers (magnetic tapes), HMS uses IBM's data encryption hardware and software technologies.

ENCRYPTION

HMS's encryption policy provides guidance on the use of communication resources, cryptographic controls, exchange agreements with other organizations, and ways that ensure that sensitive data is properly controlled on systems available to the public. HMS ensures that exchange of information will be protected by adequate controls and that all of our communication resources will be used for business purposes only. Our encryption policy provides direction on its use and other controls and includes:

- Use of encryption—establishes requirements for determining when encryption is required:
  - Authorization for the use of encryption solutions
  - Encryption on laptops
  - Encryption to protect sensitive information
  - Ownership of encryption implementation
  - Review of encryption implementation
  - Satisfaction of legal requests
  - Use of digital certificates
  - Use of encryption products outside the United States
  - Wireless access authentication and encryption
- Digital signatures—establishes requirements for the use of digital signatures:
  - Confirming the use of digital signatures
  - Using digital signatures
  - Using nonrepudiation services

- Key management—establishes requirements for the management and protection of encryption keys:
  - Compromising of encryption keys
  - Recovering encryption keys
  - Escrow of encryption keys
  - Managing encryption keys
  - Renewal and expiration of encryption keys

File Exchange

Momentum Systems' Secure Network Gateway provides workflow-driven managed file transfer software that secures, simplifies, and automates the exchange of files between HMS and AHCCCS. Secure Network Gateway establishes an easily scalable automated file transmission gateway, thus lowering the cost of managing and administering file communication. The Secure Network Gateway also creates an automatic flow of files between HMS applications and AHCCCS and delivers automatic confirmations and notifications of receipt.

The Momentum hardware/software file transfer solution allows for the use of scripting to automate the above processes. Files can automatically be received and transmitted—and this activity can be logged, including business notification of the process completed—without human intervention. Exception reporting and notification is generated whenever any process falls outside of a predetermined set of conditions.

All inbound, client-initiated transfers are directed to the Momentum Gateway server, and transfers initiated by HMS are handled by the Momentum AFD server directory.

Data at Rest (Stored)

HMS policies for stored data meet AHCCCS's security requirements. Confidential healthcare data at rest on computer systems owned by and located within HMS's controlled spaces and networks is protected by at least one of the following:

- Encryption
- Firewalls with strict access controls that authenticate the identity of those individuals accessing the HMS Network
- Securing the data requiring protection during storage to prevent unauthorized exposure. All data is secured within a physical space that is controlled and managed by an electronic key card system
- Other compensating controls, including complex passwords and physical isolation/access
- HMS password policies and guidelines stating that password protection is not an acceptable alternative to protecting confidential PHI data if used alone but when combined with all controls, including encryption, is a viable security method
- Data server segregation by company

Portable devices may contain data at rest. Many incidents involving unauthorized exposure of confidential or PHI data are the result of stolen or lost Portable Computing Devices (PCDs). The most effective means to prevent these exposures is to avoid storing confidential data on those devices. As a general practice, confidential client data must not be copied to or stored on a PCD. However, in limited situations that require storing confidential or client-sensitive data on such devices, encryption reduces the risk of unauthorized disclosure if the device is lost or stolen.

Offsite Data Storage

HMS backs up all critical AHCCCS data in accordance with State specifications to ensure a successful recovery of our business applications. We back up and secure all critical data for offsite storage and disaster recovery access use, as required. We perform both full-volume back-ups and incremental file back-ups of all data storage and LAN file server devices.

As noted above, HMS currently uses Iron Mountain for offsite data back-up repository; storage of paper copies of documentation, manuals, tape media, and other hardcopy materials related to our services; and vital record management. All vital records are secured at Iron Mountain's record retention facility, and the Record Storage Tracking Database tracks and manages them.

All file types indicated in the Critical Systems Files Determination list must be backed up and sent to offsite storage on a defined schedule to ensure that business applications and systems can be recovered without impacting client recovery capabilities and to comply with auditing and legal requirements.

For offsite data back-ups, only authorized data center management is given unique authorization cards to enter Iron Mountain data storage facilities and to access SecureSync, the web-based management facility. As a mandate, access passwords must be changed every six months unless the employee leaves HMS, in which case we immediately revoke access.

Iron Mountain implements stringent security controls and limits access to client information to only personnel authorized by its clients, including HMS. We regularly visit the offsite storage location to ensure that our materials are stored and protected at the highest level of safety, security, and quality that we expect from Iron Mountain. All site visits to facilities must be scheduled and approved by two of the authorized HMS "validating contacts" on file with Iron Mountain.

Release of Information

HMS understands the critical importance of safeguarding client information. It is HMS's policy not to release any information to any party without receiving prior written approval from our clients, including AHCCCS. Likewise, HMS will communicate with State counsel if necessary regarding such matters if the situation warrants.

Monitoring Suspect Activity

HMS maintains a long-standing program of surveillance and in monitoring for suspect activity. Our company has stringent audit controls in place, and we will track a suspect situation from the onset of the suspicious activity through resolution. HMS's CSO, Human Resources (HR) department, and CCO work

in tandem to identify, analyze, diagnose, and resolve any such situation based on a pattern of suspected anomalies or irregularities in performance or actions of an individual or situation. If we confirm that an employee has engaged in intentional suspect activity, HMS will immediately terminate that employee.

Restricting Access to Facilities

It is our company policy to limit access to sensitive information to only personnel authorized to access specific data. To ensure the protection of client information:

- All HMS locations require key card access entry to all floors and suites.
- All employees are required to wear on the outside of their apparel picture ID badges confirming their identity and employment.
- Security cameras are installed at various points of entry in our offices so authorized HMS personnel can monitor activity
- All visitors are required to sign in and out at the reception desk, wear an ID badge clearly indicating they are a visitor to our facility, and wait for an HMS employee escort to assist them to the department that they intend to visit

Audit Controls to Monitor Physical and System Access

HMS has an effective suite of audit trails and controls in place to trace both physical and system access and to discover attempts at unauthorized access. As stated previously, HMS requires that all employees wear ID badges, maintains secured entry points at all locations that require key card access, and uses security cameras to monitor employee or visitor activity as well as access at all locations. Attempts at unauthorized access are documented and appropriate actions taken.

To ensure that client information is safeguarded, our audit control methods include:

- Reviewing our processes on a regular basis to determine their effectiveness and enhancing them if needed
- Conducting monthly internal audits for both physical and logical access
- Producing reports by each authenticating system
- Conducting samplings to ensure compliance

HMS uses Compliance Insight Manager, a software tool that provides a security overview with automated, enterprise-wide compliance and activity monitoring. HMS monitors and audits privileged users for databases, applications, servers, and mainframes and reviews the data on a monthly basis. All gathered information is reviewed, documented, and presented at our monthly Security Committee meetings.

Tracking and Documenting Security Updates

As part of our internal audit processes, we date-stamp all documented security protocols to indicate the date on which they were originally written and approved. Similarly, HMS conducts regularly scheduled reviews of policies and procedures, quarterly at a minimum, and as we update or enhance security policies, we emboss the date of the revision or update on the document itself, acknowledging the date on which the change was made.

This page intentionally left blank.