AHCCCS
Arizona Health Care Cost Containment System

INFORMATION TECHNOLOGY PLAN

(IT Plan for FY2015 – FY2019)

September, 2014
Thomas J. Betlach, Director
James Wang, CIO

AHCCCS
801 East Jefferson Street
Phoenix, Arizona 85034
(602)417-4000
www.azahcccs.gov

Contents

Information Technology Trends

The following are major trends that impact the Agency's strategic planning for information technology: Security, Big Data and Analytics, Cloud Computing, Health Information Technology, Mobile Devices and Applications, and Flexible Work Environment.

Security

As more applications are delivered via a web of connectivity and users increasingly access them remotely from their personal devices, security concerns and risk management rise to the forefront.

Information security must protect information throughout the life span of the information, from the initial creation of the information on through to the final disposal of the information. This is an ongoing process of exercising due care and due diligence to protect information, and information systems, from unauthorized access, use, disclosure, destruction, modification, or disruption or distribution. It involves ongoing training, assessment, protection, monitoring & detection, incident response & repair, documentation, and review.

The process of risk management is also an ongoing, iterative process. It must be repeated indefinitely. The business environment is constantly changing and new threats and vulnerabilities emerge every day. In addition, the choice of countermeasures or controls used to manage risks must strike a balance between productivity, cost, effectiveness of the countermeasure, and the value of the informational asset being protected.

For any given risk, management can choose to accept the risk based upon the relative low value of the asset, the relative low frequency of occurrence, and the relative low impact on the business. Or, leadership may choose to mitigate the risk by selecting and implementing appropriate control measures to reduce the risk. In some cases, the risk can be transferred to another business by buying insurance or outsourcing to another business. The reality of some risks may be disputed. In such cases leadership may choose to deny the risk.

For example, organizations are permitting employees to bring personally owned mobile devices (laptops, tablets, and smart phones) to their workplace, and to use those devices to access privileged company information and applications which adds to their risk. More and more users and businesses use smartphones as communication tools but also as a means of planning and organizing their work and private life. Within companies, these technologies are causing profound changes in the organization of information systems and therefore they have become the source of new risks. Indeed, smartphones collect and compile an increasing amount of sensitive information to which access must be controlled to protect the privacy of the user and the intellectual property of the company.

All smartphones, as computers, are preferred targets of attacks. These attacks exploit weaknesses related to smartphones that can come from means of communication like SMS, MMS, Wi-Fi networks, and GSM. There are also attacks that exploit software vulnerabilities from both the web browser and operating system. Finally, there are forms of malicious software that rely on the weak knowledge of average users.

Different security counter-measures are being developed and applied to smartphones, from security in different layers of software to the dissemination of information to end users. There are good practices to be observed at all levels, from design to use, through the development of operating systems, software layers, and downloadable apps.

Big Data and Analytics

Big data is high volume, high velocity, and/or high variety information assets that require new forms of processing to enable enhanced decision making, insight discovery and process optimization. Big data is difficult to work with. It brings with it challenges – in storing it and in integrating it all into a form that can be used for business tasks.

Analytics is closely associated with big data as analytics are necessary to derive insights usable for decision-making from big data – data exploration, predictive analytics, query and reporting, data discovery, forecasting, planning and what-if analysis. Before analytics can provide value, the big data it operates on must be integrated and processed, and end results must be consistent and dependable.

Best results require confidence with accurate timely data, common definitions for key business terms, and transparency – must be able to trace path through systems to know where data came from and how it was manipulated. Start with data you trust at data creation, test data quality, apply data cleansing. Confidence in data quality enables confidence in analytics results.

Big data needs to be integrated. Both IT and business users need to participate in data integration – developing standard names, metadata that can be shared across all data sources, establish rules for processing and routing data, join disparate data sources during transformation.

Performance is key – data changes rapidly and must be fed to various applications in system quickly so that leaders can react to changing conditions as soon as possible. Consider scalability across all architectures, load balancing, cross platform support, development and testing environments, scalable execution of tasks, mobile access to monitor data integration. Deliver data appropriately – achieve high performance and scalability for real-time processing as well as batch

More data may lead to more accurate analyses – more accurate analyses may lead to more confident decision making, and better decisions can mean greater operational efficiencies, cost reductions, and reduced risk.

Cloud Computing:

Cloud computing is Internet-based computing of dynamically scalable and often virtualized resources. These resources are broadly divided into three categories:

- Infrastructure-as-a-Service (IaaS) provides virtual server instances with unique IP addresses and blocks of storage on demand. Customers use the provider's application program interface (API) to start, stop, access and configure their virtual servers and storage.
- Platform-as-a-Service (PaaS) as a set of software and product development tools hosted on the provider's infrastructure. Developers create applications on the provider's platform over the Internet. PaaS providers may use APIs, website portals or gateway software installed on the customer's computer.
- Software-as-a-Service (SaaS), the vendor supplies the hardware infrastructure, the software product and interacts with the user through a front-end portal.

A cloud can be private or public. A public cloud sells services to anyone on the Internet. A private cloud is a proprietary network or a data center that supplies hosted services to a limited number of people.

Health Information Technology:

The nation's healthcare system is being transformed through the adoption of technology for patient health records, exchange of health information, patient monitoring and care delivery, health outcomes analytics and measurement in an effort to improve quality, safety and efficiency of care.

Broad and consistent utilization of HIT will:

- Improve health care quality or effectiveness;
- Increase health care productivity or efficiency;
- Prevent medical errors and increase health care accuracy and procedural correctness;
- Reduce health care costs;
- Increase administrative efficiencies and healthcare work processes;
- Decrease paperwork and unproductive or idle work time;
- Extend real-time communications of health informatics among health care professionals; and
- Expand access to affordable care.
- Early detection of infectious disease outbreaks around the country;
- Improved tracking of chronic disease management; and

- Evaluation of health care based on value enabled by the collection of de-identified price and quality information that can be compared.

Mobile Devices and Applications

More and more applications are going mobile combined with cloud computing to make mobile applications a prime delivery mechanism. A mobile computing device has an operating system (OS), and can run various types of application software, known as apps. Most devices can also be equipped with Wi-Fi, Bluetooth, and GPS capabilities that can allow connections to the Internet and other Bluetooth-capable devices, such as an automobile or a microphone headset. A camera or media player feature for video or music files can also be typically found on these devices along with a stable battery power source.

A mobile app, short for mobile application or just app, is application software designed to run on smartphones, tablet computers and other mobile devices. Mobile apps were originally offered for general productivity and information retrieval, including email, calendar, contacts, and stock market and weather information. However, public demand and the availability of developer tools drove rapid expansion into other categories, such as mobile games, factory automation, GPS and location-based services, banking, order-tracking, and ticket purchases.

Developing apps for mobile devices requires considering the constraints of these devices. Mobile devices run on battery and have less powerful processors than personal computers. Developers also have to consider a lengthy array of screen sizes, hardware specifications and configurations because of intense competition in mobile software and changes within each of the platforms. Mobile application development requires use of specialized integrated development environments. Mobile apps are first tested within the development environment using emulators and later subjected to field testing. Emulators provide an inexpensive way to test applications on mobile phones to which developers may not have physical access.

Mobile application management (MAM) describes software and services responsible for provisioning and controlling access to internally developed and commercially available mobile apps used in business settings, which has become necessary with the onset of Bring your own device (BYOD) phenomenon. When an employee brings a personal device into an enterprise setting, mobile application management enables the corporate IT staff to transfer required applications, control access to business data, and remove locally cached business data from the device if it is lost, or when its owner no longer works with the company.

Flexible Work Environment

Flextime permits workers to vary their schedule. For example, they may opt to work four 10-hour days per week, taking Monday or Friday off. Other workers may opt simply to come in early, such as 5 or 6 a.m., and leave in the mid-afternoon, or come in late and therefore leave late. One benefit of such a schedule is that commuting times occur outside of the congested

rush hour traffic within a given geographic region. Flextime arrangements also help parents: one parent works 10 a.m. - 6 p.m. and is in charge of the children before school / daycare, while the other parent works 7 a.m. - 3 p.m. and is in charge of the children after school / daycare. This allows parents time to commute. Flextime is also beneficial to workers pursuing an education.

Virtual office and telework programs allow workers to perform their work from home, either permanently or periodically. Working from home eliminates the commute time and the cost of transportation.

BYOD is making significant inroads in the business world. Some believe that BYOD may help workers be more productive, and others say it increases morale and convenience by using their own devices and makes the company look like a flexible attractive employer. Many feel that BYOD can even be a means to attract new hires.

All of these are an ongoing part of the work-life balance discussions in many companies.

Information Technology Issues

The unsettling economic climate, the speed with which technology evolves, and the increasing occurrence of unauthorized network attacks impact the future of information technology and must be considered in IT planning.

Security

With the speed of change in software, hardware, and applications plus the spread of exploit deployment, the Agency recognizes the need to perform a continuous enterprise-wide lifecycle of vulnerability discovery and remediation. Perimeter defenses such as anti-virus and firewalls are vital, but can be bypassed by determined effort to reach and exploit *known* vulnerabilities that reside just inside the fence. Nearly all data loss events resulting from an outside attack, and most losses to insider attack, consist of the exploit of a *known*, but unhandled vulnerability. Current best practice indicates that this is best answered by performing regular vulnerability assessments to identify/remediate the known vulnerabilities in a network before hackers find them.

During the past year AHCCCS has performed four vulnerability assessments, and has purchased an assessment tool in order to run frequent self-assessments. The majority of the assessment findings have been mitigated, with the remainder in process. AHCCCS plans to be diligent and attentive to vulnerability discovery and remediation so as to protect and safeguard the data entrusted to the Agency by its members and maintain a high level of security.

AHCCCS has set the following goals to address security:

- Compliance with Statewide Security Policies and Standards as continually updated
- Conformance with Health Insurance Portability and Accountability Act (HIPAA) that establishes privacy and security guidelines for the protection of IT assets and resources, including data and information
- Network is resilient and available to support agency-critical applications
- Periodic security assessments and remediation including process/procedure, vulnerability, and penetration
- Data integrity is maintained
- Maintain network infrastructure by applying patches and updates regularly
- Threat protection, threat management, monitoring and mitigation are in place
- Executive Order 2008-10, endeavor to protect confidential information it acquires from its citizens and businesses through the deployment of encryption technologies

Staff Retention

Government is losing its attractiveness as a stable work environment. Shrinking state revenues in recent years have forced governments to lay off workers, reduce salaries, close offices, issue furlough days, and increase out-of-pocket expenses for health care, retirement, and state tax.

Today, hiring and retention is being affected by the acceleration in private sector hiring. At the same time, government is challenged to enhance its mission critical mainframe systems according to new legislative requirements such as Health Care Reform, while the mainframe workforce is shrinking and younger workers have little motivation to learn mainframe technologies.

AHCCCS is addressing these problems by offering a flexible work environment where employees can choose an alternative work schedule or work site, employees are recognized, work assignments are prioritized and aligned with agency plans, documentation and change control are expected, and cross-training and succession plans are the norm.

Technology Refresh

The typical lifecycle of network infrastructure and end user hardware and software is three to seven years as long as patch management is practiced regularly. A significant investment is required to maintain this schedule and government agencies often forego technology refresh in favor of other priorities.

AHCCCS has been aggressive in its effort to lessen the impact of technology refresh by virtualizing its servers and replacing PCs with Thin Client devices, but even the supporting infrastructure needs to be refreshed at some point. The agency continues to plan for regular technology refresh and has been successful during the past three years to replace many of the aging devices.

In addition to the network infrastructure, application systems also age and their technology become obsolete. Replacing such applications requires time and money. The mission critical PMMIS was built on 1980 technology (CA IDEAL using CA DATACOM database) and took more than five years for design, development and implementation. The cost exceeded $50 million. PMMIS was implemented 24 years ago in 1990. Covered recipients have grown from 400,000 to 1.5 million.

FY2014 Accomplishments

1. Security Enhancement
    a. Completed independent vulnerability assessment and penetration testing
    b. Completed the SSAE-16 security audit (process and procedure)
    c. Upgraded web server firewalls
    d. Consolidated data center with State facility (ADOA)
2. Technology Refresh
    a. Replaced end of life servers, load balancers, storage filers
    b. Upgraded and merged telephone system with State system
3. Agency Business Functions
    a. BHS integration
    b. HEAplus implementation
4. Health Information Technology (HIT)
    a. Implement Stage 2 Meaningful Use (MU) for Medicaid EHR Incentive Program

Agency Business Goals

1. AHCCCS must pursue and implement long term strategies that bend the cost curve while improving member health outcomes.

2. AHCCCS must pursue continuous quality improvement.

3. AHCCCS must reduce the systematic fragmentation that exists in healthcare delivery to develop an integrated system of healthcare.

4. AHCCCS must maintain core organizational capacity and workforce planning that effectively serves AHCCCS operations.

IT Vision

Information … when, where, and how you need it!

IT Mission

To provide, operate, maintain and support high quality information systems to enable AHCCCS to continue to be a leader in providing comprehensive quality health care to those in need.

Goal 1

Maintain IT infrastructure to support Agency business functions and goals

Objectives

- Technology refresh [replace aging hardware, upgrade to current versions of software]
  - Upgrade all Windows 2003 servers to 2008 or 2012 [start with web servers]
- Maintain and operate applications, web presence, imaging [includes purge process]
- Maintain hardware/software [renew service agreements and licenses]
- Provide and maintain contracts for SAAS [program integrity, HEAplus]
- Implement application performance management tools

Performance Measures

PMMIS System Availability	Target FY2014	Actual FY2014	FY2015	FY2016	FY2017
	99.5%	99.75%	99.5%	99.5%	99.5%

Network System Availability	Target FY2014	Actual FY2014	FY2014	FY2015	FY2016
	99.5%	99.83%	99.5%	99.5%	99.5%

Goal 2

Utilize best practice technologies that enhance and improve efficiency and effectiveness of Agency business functions and goals

Objectives

- Cost Sharing by 10/1/2014
- DRG (Payment Reform) by 10/1/2014
- HIT/HIE Enhancement for Stage 2 MU by 10/1/2014
- ICD-10 by 10/1/2015
- AFIS replacement (BREAZ) by 10/1/2015
- Greater Arizona by 10/1/2015
- HEAplus Additional Rollout by 12/31/2015
- Data Analytics for OIG by 12/31/2015
- Data Warehouse/Decision Support System Enhancement by 12/31/2015
- 999 Lines by 01/01/2016
- Asset Tracking System by 6/30/2016
- Improve the quality of software that ISD delivers for our customers through continuous process improvement in a practical, efficient, and value driven manner
- Plan PMMIS and HPMMIS replacement strategies
- Infrastructure Enhancement (reliability, resiliency, consistency)

Performance Measures

Number of Key Project Milestones Met	Target FY2014	Actual FY2014	FY2015	FY2016	FY2017
	250	175*	100	100	100

*Milestone definition changed during this timeframe

Goal 3

Proactively protect Agency data

Objectives

- Regular security audits and remediation
  - Conduct monthly vulnerability scanning and remediation (Shavlik and Metasploit tools)
  - Conduct annual third party security auditing and remediation

- Threat and risk management and mitigation
  - Implement XenMobile application for mobile devices
  - Implement weekly patching program
  - Implement data at rest encryption solution
  - Implement secured email solution
  - Implement 2-factor authentication (security dongles) for external users with access to PHI
- Backup and recovery
  - Implement disk-based backup solution
- Acute system interruption notification plan
- COOP

Performance Measures

Number of Documented Findings Remediated	Target FY2014	Actual FY2014	FY2015	FY2016	FY2017
	10	11	10	10	10

Goal 4

Maintain a high-performing, innovative, and reliable/dependable workforce

Objectives

- Succession planning and cross training
- Recognition
- Training
- Flexible work environment

Performance Measures

Turnover Percentage	Target FY2014	Actual FY2014	FY2015	FY2016	FY2017
	15%	13.95%	15%	15%	15%