Trusted Health IT and IT-as-a-Service: A Prescription for Change

Save to myBoK

By Roberta Katz, Director, Healthcare Solutions,EMC Corporation, @Roberta_Katz, @EMCHealthcare

Healthcare organizations are increasingly reliant on electronic health records (EHR) for patient care collaboration with trusted IT becoming a key requirement to share protected health information (PHI).

Trusted IT solutions for Health Information Management (HIM) typically include advanced security, integrated backup and recovery, and continuous availability as part of the supporting IT architecture. Healthcare providers face the unique challenge of keeping PHI highly-available, secure, and private as they increase caregiver access via mobile, social, cloud, and Big Data tools to improve patient care delivery.

Security breaches—whether the data is kept on physical IT assets or in a private/hybrid cloud—can create a lack of confidence in a healthcare system along with significant regulatory implications. Although many healthcare organizations plan to conduct and/or deploy remediation coming from a HIPAA security risk assessment, a core requirement of stage 2 of the “meaningful use” EHR Incentive Program there is more work to be done.

The HIM Diagnosis

Many organizations are implementing IT-as-a-Service (ITaaS) to lower costs, improve service levels, and accelerate key application deployment. To gauge progress in healthcare environments and capture lessons learned, MeriTalk released the Rx: ITaaS + Trust report, underwritten by EMC, which includes the perspectives of more than 300 health IT executives on the topic.

The results show that in the last 12 months, 61 percent of global healthcare organizations have experienced a security-related incident in the form of a security breach, data loss, or unplanned downtime at least once. These breaches, data loss, and unplanned outages experienced at hospitals with 100 beds and above cost US hospitals more than $1.6 billion annually. Additionally, the study found:

- **Security Breaches:** Nearly one in five (19 percent) global healthcare organizations has experienced a security breach in the last 12 months at a cost of $810,189 per incident. Health IT executives say the most common causes for breaches include malware and viruses (58 percent); outsider attacks (42 percent); physical security—loss/theft of equipment (38 percent); and user error (35 percent).
- **Data Loss:** Nearly one in three (28 percent) global healthcare organizations has experienced data loss in the past 12 months at a total cost of $807,571 per incident. And, of those, more than a third (39 percent) have experienced 5 or more incidences of data loss in the past 12 months. Common causes of data loss include hardware failure (51 percent); loss of power (49 percent); and loss of backup power (27 percent).
- **Unplanned Outages:** Almost two out of five (40 percent) global healthcare organizations have experienced an unplanned outage in the past 12 months at a cost of $432,000 per incident. On average, healthcare organizations have lost 57 hours to unplanned downtime over the past 12 months. The most common causes of outages include hardware failure (65 percent); loss of power (49 percent); software failure (31 percent); and data corruption (24 percent).

Failing to invest in trusted IT solutions to protect data and ensure a reliable, highly-available infrastructure can result in real quantifiable costs to a healthcare system. In addition to the financial implications, inefficient IT architecture can slow the transition many organizations are making as they deploy IT-as-a-Service (ITaaS) models and seek to deliver IT solutions to other organizations inside and outside of their network. ITaaS models help organizations increase agility, accelerate deployment of key healthcare applications, and lower costs.

Healthcare organizations are in the process of complying with HITECH requirements for privacy and security of PHI. Failure to adhere to the requirements means providers sacrifice significant federal funding available for meaningful use incentives. Yet, within the US, less than one in three respondents (27 percent) believe their organization is fully prepared to ensure continuous availability of electronic PHI (ePHI) during unplanned outages, disaster recovery, or emergency mode operations.

Just 18 percent say their technology infrastructure is fully prepared for a disaster recovery incident.

Prescription for Change

So Where do healthcare organizations go from here? Looking to the future, "Rx: ITaaS + Trust" highlights that 88 percent of organizations are preparing to become the "IT service provider of choice" within their own networks. Popular steps include:

- Upgrade information security – 66 percent
- Define goals and objectives – 63 percent
- Define a governance process for IT services – 56 percent
- Build/confirm senior leadership support – 52 percent

In addition to preparing, organizations are planning investments in:

- HIPAA Security Risk Analysis as part of EHR meaningful use requirements – 46 percent
- Single Sign On and authentication for Web-based applications and portals – 44 percent
- Audit tools and log management – 43 percent
- Encryption for protected health information – 42 percent

Healthcare organizations are encouraged to take a holistic view of security management by adopting an integrated approach to governance, risk, and compliance (GRC). To align appropriate security activities for maximum protection across the enterprise, a key step is integrating a security management framework into the IT infrastructure comprised of:

- **Business governance:** Embedding security into all organizational structures and processes while taking into account regulatory requirements (HIPAA, HITECH) and internal policies
- **Security risk management:** Identifying and classifying information risks and tracking risk mitigation
- **Operations management:** Implementing security processes and controls in line with security policy to prevent risks from developing into security incidents
- **Incident management:** Detecting, analyzing, resolving, and reporting security incidents to minimize their impact

While these strategies can be implemented using a phased approach, investing in a secure and reliable IT architecture increases trust in IT while improving patient care delivery. Key ITaaS technology enablers include a cloud-based, highly automated technology infrastructure, as well as an online catalog of standardized business, IT, and clinical services that clinicians and administrators can directly consume. These technologies will enable healthcare organizations to significantly improve their HIM infrastructure while maintaining available, secure, and private PHI across the board.

Original source:
Katz, Roberta. "Trusted Health IT and IT-as-a-Service: A Prescription for Change" (Journal of AHIMA), August 2014.