Mobility Security Strategy: Lifeline for Next Generation Healthcare

Executive Summary

Mobile devices extend the wired infrastructure, increasing the overall risk to organization networks. The balance between information protection and information access becomes more complex as the availability of mobile devices increases. To cope with the challenges introduced due to the adoption of mobility in healthcare, strategic imperatives to support a mobile and wireless healthcare ecosystem must be developed and thoroughly explored.

at&t

The Move from Paper to Bits and Bytes

With the passage of the HITECH Act (Health Information Technology for Economic and Clinical Health), healthcare organizations are encouraged to move towards electronic healthcare records and online availability of information.

The HITECH Act is part of the American Recovery and Reinvestment Act ("ARRA"), which allocated approximately $25 billion[1] to modernize health information technology (Health IT/HIT). The HITECH Act also stipulates new HIPAA privacy, security and protection requirements to advance the secure use of HIT. An important goal of the Act is to preserve the integrity of Protected Health Information (PHI) and Personally Identifiable Information (PII), making the information electronically available while ensuring the confidentiality of the information in order to increase efficiency, accuracy and quality of health services.

We are all familiar with the unique challenges of the healthcare industry related to rising costs, the aging demographic, emerging diseases and the demand to deliver higher quality healthcare efficiently and in a cost effective manner. To meet these demands, healthcare organizations have begun to use mobile devices within their organization. While this trend helps increase efficiency, quality, and overall delivery of healthcare services, it is leading to a movement away from a traditional paper-based model for data towards electronic information access and availability.

Compliance and Regulatory Demands

The development of a revamped mobile electronic health information infrastructure and the sharing of health information for patient care and medical research offer enormous promise to improve healthcare and promote innovation. However, this expanded information sharing and innovation also raises risks related to patient privacy and confidentiality. Not only do the regulations such as HIPAA and HITECH and industry best practices such as HITRUST and ISO 27001 require that health care provider organizations have security and privacy safeguards in place, but consumers also demand protection of their health information.

The ultimate goal in moving towards Mobile Health is to provide the best care to the patient which requires accessibility of information on the go. Adopting this technology raises security and privacy concerns.

Importance of Security Coverage

The rapid and enthusiastic adoption of mobile technology in the healthcare industry comes as no surprise. This is an industry that, while steeped in tradition, is also driven by discovery and innovation. Healthcare professionals are routinely and increasingly using mobile devices to access and review patient records and test results, enter diagnosis and billing information during patient visits, consult drug formularies and other reference material and synchronize information with their organizations' centralized systems, all without the need for wired network connections.

Healthcare organizations must keep a very close eye on the emerging wireless mobility marketplace as there is a tremendous growth in new technology and capabilities. The number of vendors offering wireless services and products is overwhelming and with new announcements daily, navigating the landscape can be challenging.

It is essential for a healthcare organization to align the wireless technology with their existing business processes to achieve the desired objectives of a mobile healthcare infrastructure. These mobile devices are replacing desktops and wired phones to augment both voice and data application access to personnel within the expanding organization. A critical area of concern is information security and patient personal information privacy.

To enable effective and secure information sharing, healthcare organizations require a clear, consistent ability to identify sensitive information and determine proper handling. This is achieved by developing a mobile device management security strategy. It is important to use a well thought out security strategy rather than just plain technology to meet your security needs. Strategy involves people, process and technology to provide a holistic security framework for your organization.

Security Strategy for a Fading Boundary

Mobile devices and the sensitive information they contain must be managed and protected. The flow of information is in line with the patient's mobility, starting at the doctor's office and moving to laboratories, imaging centers and other care facilities. This natural mobility provides many points of exposure for information security breaches. The requirements for secure organization architecture are changing with the increasing interconnection between hospitals and clinics, physician remote offices and healthcare associates. As a result, security perimeters must expand beyond the internal network to numerous critical endpoints.

Mobile Device Management

Mobile device management within organizations becomes more complex and important as both the number of devices and the amount of sensitive data reaching them increases. Part of the risk is that devices may get lost or stolen, potentially compromising stored critical data unless there are processes and tools in place to protect it.

Mobile Device Asset Discovery and Inventory

The first step in securing the mobile organization network is identification of the current inventory of mobile devices and OS clients that exist within your infrastructure. Next, you must integrate the mobile devices that have been identified in this process into your existing asset inventory database. This will help with Mobile Device Management. When developing or updating your mobile device asset inventory, consider the following:

a. How will you identify the mobile assets?

b. What are the related assets to this mobile device, for example, additional memory cards?

c. Identify the asset owner to whom this device has been assigned and possibly its business purpose.

d. How are you going to keep this asset inventory updated?

e. Plan on categorizing the mobile assets by hardware, OS, deployment date, etc.

Business Process Profiles

The flow of mobile health information is characterized by portable hardware coupled with software applications and patient data across wireless networks. Mobile health enables clinical access to a variety of major software applications central to patient care and subsequently increases clinicians' reach, mobility and ease of information access, regardless of location. For example, a clinician might use a mobile device to access a patient's electronic health record (EHR), write and transmit prescriptions to a pharmacy, interact with patient treatment plans and communicate public health data, order diagnostic tests,

review labs, or access medical references. Data transmission is realized by technologies common in everyday life including bluetooth, cell phone, infra-red, wi-fi and wired technologies, all of which operate as part of a network.

In this step, organizations need to identify the existing business processes and what type of processes would most benefit from the use of mobile technology. They should identify the needs for remote data access and profile the available devices to map their capabilities to the functional requirements of the processes identified. This will permit a mapping of mobile device capabilities to the associated business processes, network access requirements and transport mechanisms.

Risk Assessment

It is important for organizations to understand their current infrastructure and evaluate the threats that can occur if mobile devices are incorporated. Once threats have been identified, the next step is to look at the impact of these threats. The comprehensive risk assessment process must be an ongoing effort to ensure that the risks of the evolving threat landscape are addressed. This risk assessment provides a better picture of the potential exposures and associated risks.

Mobile Device Security Policy

Organizations need to identify and develop mobile security policies to be deployed and which will provide adequate protection. These policies should ensure that the many regulatory or compliance concerns that might be applicable are addressed. The mobile security policy should be integrated within your overall information security policy framework.

Key elements to address in the mobile device security policy are:

- Physical security of the device
- Address lost or stolen devices
- Acceptable uses of the device
- Encryption
- Password protection
- Storage
- Backup
- Access Control
- Authentication
- Monitoring

Like every other security policy, an organization must regularly review its mobile device security policy, particularly after the acquisition of new mobile devices, configuration changes and in the wake of security incidents involving mobile devices.

Mobile Application Security

Mobile applications extend traditional network boundaries and introduce new avenues of attack. They often provide access to sensitive business and personal information. They are constantly challenging and extending their reach. Organizations need to ensure that a secure coding process is followed while building mobile applications and should include security testing as part of the Software Development Life Cycle (SDLC) process.

Security Awareness

Organizations need to raise awareness about how each employee can protect an organization's confidential and sensitive information (including electronic information) and their own personal information. It is important that awareness programs be developed to help staff better understand and reduce the risks of using laptops and other mobile devices.

Conclusion

The transforming healthcare IT landscape is an exciting development in the industry. There are huge opportunities for mobility to provide an advanced solution to address healthcare information challenges. This opportunity also demands a multi-level security strategy and framework encompassing technical, organizational and regulatory factors to stay ahead of the security curve. Proactively introducing a mobile security strategy to tackle the growing challenges associated with mobile device security can go a long way towards building and revamping the current healthcare infrastructure towards a more secure health IT.

Notes

1. http://www.recovery.gov/Transparency/agency/Recovery%20Plans/HHS%20Recovery%20Act%20Plan%20-%20June%202010.pdf

For more information, contact an AT&T representative or visit www.att.com/consulting/security.

09/30/10 AB-1979

at&t