Trends for the Mobility-Enabled Healthcare Enterprise and Security Threats, Vulnerabilities, and Countermeasures

NIST HIPAA Conference
May 10, 2011
Agenda

- Context for Mobile Health

- Risks

- Security Implementation Considerations
Health care has increasingly used technology to expand its reach or enhance delivery

- Hippocrates (460-377 B.C) and Galen (131-201 A.D) documented their patient’s process of healing to improve patient care.
- 1901 the Trans-Atlantic radio introduced and by 1924, envisioned this technology bringing the doctor to our home.
- 1946 the ENIAC computer introduced.
- 1950 the transmission of radiologic images by telephone between West Chester and Philadelphia (24 miles was reported in the scientific literature).
- 1970s a growing number of electronic medical records systems were introduced.

Rapid advancements of today bring even more possibilities tomorrow.

Ready for what’s next
Today, mobility and “anywhere connectivity” is being used to transform business, drive productivity, and redefine the workplace.
The explosion of new devices and applications focused on healthcare solutions is resulting in mHealth...

...a term used for the practice of medical and public health, supported by mobile devices
These mobile solutions offer significant opportunity for improvements across the health market

<table>
<thead>
<tr>
<th>Education</th>
<th>Reminders and Alerts</th>
<th>Data Collection</th>
<th>Care Delivery</th>
<th>Emergency/Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search the web for health information</td>
<td>Local alarm or calendar alerts</td>
<td>Patient History at the Bedside; home visits</td>
<td>View patient information, labs, images</td>
<td>Collect and transmit patient data at the point of care</td>
</tr>
<tr>
<td>Utilize local software or remote enterprise applications</td>
<td>Register for service – calls; text messages</td>
<td>Personal Health Records… local or hosted</td>
<td>Remote monitoring &amp; consults</td>
<td>Transmit images from the scene</td>
</tr>
<tr>
<td>Conduct patient education or review results bedside</td>
<td>Enter information for personalized responses</td>
<td>Door to door surveys and research protocol data collection</td>
<td>Prescription ordering</td>
<td>Obtain guidance and start intervention</td>
</tr>
</tbody>
</table>

Examples:

- Search the web for health information
- Utilize local software or remote enterprise applications
- Conduct patient education or review results bedside
- Local alarm or calendar alerts
- Register for service – calls; text messages
- Enter information for personalized responses
- Patient History at the Bedside; home visits
- Personal Health Records… local or hosted
- Door to door surveys and research protocol data collection
- View patient information, labs, images
- Remote monitoring & consults
- Prescription ordering
- Dictation
- Clinical Decision Support
- Collect and transmit patient data at the point of care
- Transmit images from the scene
- Obtain guidance and start intervention

Readied for what’s next
Success of these mobile solutions requires a holistic and integrated approach

Clinical Integration

Usability

Security and Privacy

Sustainability
As users increasingly rely on mobility for health care services, the risk of data compromise escalates.

Potential Threats and Vulnerabilities

- Device Loss
- Unsecured Wireless
- Malware Attacks
- Location Tracking
- Threats to the Enterprise

Enterprise Resources → Protection Needs → Vulnerabilities
• Context for Mobile Health

• Risks

• Security Implementation Considerations
As security professionals, we have been playing catch-up by trying to learn, analyze, and secure mobile technologies.

- Realize substantial savings, increased information dissemination from previously disparate systems, and enhanced real-time and operational efficiencies
- Ability to integrate communications more closely with business processes
- Anywhere and anytime access to email, calendars, and applications
- Enabled business processes applications with automated alerts and context-driven architectures

Increasing Security Posture

Grassroots Mobility → Ad Hoc Mobility → Structured Mobility → Optimized Mobility
Mobile technologies extend the wired infrastructure but introduce many new challenges for information security personnel

- Personal devices vs. care delivery organization (CDO)
- Connectivity from anywhere and everywhere
- Multiple devices and OS platforms
- Multiple applications to support
- Data is outside the ‘secure’ perimeter
- Hard to distribute security controls
- Access complexities (power users, etc)
- Device management
Our goal is to move employees to technologies that provide greater mobility, efficiency, and productivity

**Mobility Challenges**
- Information security concerns
- Business processes can change dramatically, presenting organizational challenges
- The business case is complex
- Point solutions that do not address total requirement
- Technical issues surrounding connectivity
- Standards are evolving
- Evolving policies and corporate governance related to mobile devices
- Human acceptance of new technology
- Integrating dynamic mobile devices with legacy information systems
- Maintaining the user experience

**Security Challenges**
- Data disclosure (storage and transmission)
- Physical security
- Strong authentication / multi-factor authentication
- Multi-user support; separate organizational and personal data
- Safe browsing
- Operating systems and abundance of hardware platforms
- Application isolation
- Malware, phishing
- Updates – App, OS, and Firmware mechanisms
- Geolocation privacy
- Improper decommissioning

**Mobile Security Considerations**
The potential effects of risk from mobility include more than just eavesdropping on mobile users

- Unauthorized **monitoring** and disclosure of ePHI
- Unauthorized **modification** of ePHI
- Unauthorized or **fraudulent** use of ePHI
- Radio frequency **interference** or disruption of service
- Radio traffic analysis and **operations** security

**In addition, mobile and wireless technology typically increases network complexity**

- Complexity is the enemy of security
- Provides more points of entry to intruders
- Mobile security tools and technologies are not standardized
So how bad is it really?

According to the Department of Health and Human Services, 9,300 medical data breaches were reported under HIPAA/HITECH between September 23, 2009 and September 30, 2010

Recent Breaches

• 18 April – Sensitive personally identifiable information (PII) was stolen from Android Skype users by malicious third-party applications
  • Any third-party application with data harvesting capabilities could steal data
    – Stolen data included customer names, date of birth, location, account balances, phone numbers, email addresses, and biographic details
• 17 March – BlackBerry JavaScript vulnerability allowed hackers to steal user data
  • Remote code execution attack provided access to media cards and storage
• 02 March – Two dozen infected applications were removed from Android Marketplace
  • Malware was capable of rooting devices and stealing data
    – Over 200,000 of these applications were downloaded
• 22 February – Financial data was stolen from thousands of Symbian and Windows mobile users
  • Zeus malware captured sensitive financial transaction authentication numbers
Implementation of mobile application technology will require integrating a number of cyber-security, privacy, and confidentiality measures.

**Mobility Security Policy and Planning**
- Establish a strong security policy foundation and risk management program for mobile solutions
- Define the mobile concept of operations (CONOPS)

**Mobility Risk Assessment**
- Assess the threats and vulnerabilities faced by the enterprise
- Define a package of security countermeasures that mitigate the risks to an acceptable level

**Mobility Security Solutions**
- Develop and integrate the applications that allow the mobile services to be secure in the enterprise
- Make engineering tradeoffs and procurement decisions
- Migrate legacy systems

**Mobility Security Operations and Administration**
- Enterprise mobile solutions are operated and administered according to defined requirements
- Security posture is periodically evaluated for compliance
• Context for Mobile Health

• Risks

• Security Implementation Considerations
The proper strategic imperatives to support a mobile ecosystem must be developed and thoroughly explored in the beginning.

<table>
<thead>
<tr>
<th>Standardization</th>
<th>Patient Safety</th>
</tr>
</thead>
<tbody>
<tr>
<td>HW and SW standardization must be considered from start to reduce maintenance costs</td>
<td>Vital factor in driving the implementation of mobility in the health care field</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Integration</th>
<th>Security</th>
<th>Asset Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integration is key to the effectiveness of system; integration with back end systems must be evaluated</td>
<td>Requirements of HIPAA, FISMA, OMB, and Privacy Act of 1974</td>
<td>Hardware and user assessment must be regularly monitored to determine overall system effectiveness and to remove defective care delivery devices</td>
</tr>
</tbody>
</table>
Successfully implementing enterprise mobility requires an advanced Secure Mobility Framework

- Implement technical policies and procedures that allow and restrict system and data access
- Unique identification, multi-factor authentication (AuthN) and role-based authorization (AuthZ) access controls
- Continuous monitoring and detection for unauthorized wireless activity
- Data encryption (at rest and in transit)
- Configuration documentation
- Physical access controls, including session/device timeouts
- Security testing and evaluation
- Conduct risk analysis
- Incorporate into Security Awareness training
- Software Assurance
Mobile security implementation includes all components of the communications system

<table>
<thead>
<tr>
<th>People</th>
<th>End-point</th>
<th>Communications</th>
<th>Perimeter</th>
<th>Enterprise</th>
</tr>
</thead>
</table>
| • Implement technical policies and procedures that allow and restrict system and data access  
• Have an approval policy and process  
• Use only approved devices and implement controls to grant/restrict remote access  
• Conduct a solution/technology risk assessment  
• Provide end user security and awareness training  
• Policy groups/role-based access | • ePHI Confidentiality/Integrity  
• Unique two-factor/PIN local and enterprise AuthN  
• Access control to local device  
• Application-level security controls  
• Device interrogation for enterprise compliance and access (phase 2 & 3)  
• Audit controls  
• Remote wipe (phase 2 & 3)  
• Data separation (personal versus sensitive)  
• Automatic logoff | • Patient History at the Bedside; home visits  
• Personal Health Records... local or hosted  
• Door to door surveys and research protocol data collection | • View patient information, labs, images  
• Remote monitoring & consults  
• Prescription ordering  
• Dictation  
• Clinical Decision Support | • Collect and transmit patient data at the point of care  
• Transmit images from the scene  
• Obtain guidance and start intervention |

Ready for what’s next
To successfully reduce risk, CDOs must extend enterprise security throughout their mobile ecosystem

The HIPAA Security Rule

- Access Control §164.312(a)(1)
- Audit Controls §164.312(b)
- Integrity §164.312(c)(1)
- Person or Entity Authentication §164.312(d)(1)
- Transmission Security §164.312(e)(1)
Security can be implemented by integrating and leveraging existing enterprise security capabilities for mobile technologies.
As with any technology, the goal is to balance convenience with security.

**Policy**
- Departmental guidance
- Roles and Responsibilities
- Security enforcement framework

**Operations Integration**
- Enrollment procedures
- System Admin Training
- Process improvement

**Technology Implementation**
- Risk Assessment
- Pilot programs
- Security overlay
- ST&E
- Certification and Accreditation
Security professionals should leverage NIST guidance and other industry best practices to establish baseline security requirements for mobile technologies

<table>
<thead>
<tr>
<th>Category</th>
<th>Control Name</th>
<th>Control No.</th>
<th>IT Policy</th>
<th>Recommended Setting</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control</td>
<td>Use of External Information Systems</td>
<td>AC-20</td>
<td>Allow Internal Connections</td>
<td>FALSE</td>
<td>Specifies whether applications, including third-party applications, can initiate internal connections</td>
</tr>
<tr>
<td>System and Communications Protection</td>
<td>Mobile Code</td>
<td>SC-18</td>
<td>Allow Resetting of Idle Timer</td>
<td>FALSE</td>
<td>Permits third-party applications to reset the inactivity timeout value, bypassing the security timeout value</td>
</tr>
<tr>
<td>Access Control</td>
<td>Concurrent Session Control</td>
<td>AC-10</td>
<td>Allow Split-pipe Connections</td>
<td>FALSE</td>
<td>Specifies whether applications, including third-party, can open internal and external connections simultaneously</td>
</tr>
</tbody>
</table>

Leverage both civil and defense policy and guidance to secure your mobile and wireless investments (i.e. CNSS, DHS, HHS, NIST, VA and DISA Wireless STIGs)
Key Initiatives and Resources…

• The HIPAA Security Rule can be found at HHS.gov: http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html

• Health information technology (Health IT) allows comprehensive management of medical information and its secure exchange between health care consumers and providers: http://healthit.hhs.gov/portal/server.pt

• The National Institute of Standards and Technology
  • SP 800-48 Rev1 - Guide to Securing Legacy IEEE 802.11 Wireless Networks
  • SP 800-97 - Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i
  • SP 800-98 - Guidelines for Securing Radio Frequency Identification (RFID) Systems
  • SP 800-111 - Guide to Storage Encryption Technologies for End User Devices
  • SP 800-121 - Guide to Bluetooth Security
  • SP 800-122 - Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
  • SP 800-127 - Guide to Securing WiMAX Wireless Communications
  • IR 7497 - Security Architecture Design Process for Health Information Exchanges (HIEs)
Closing remarks

• Don’t ignore – investigate the complete range of mobile devices necessary to enhance various clinical and business workflows within the enterprise
• Set strategy – realize that mobile and wireless technologies will create new privacy and security challenges that will require new policies and technical controls; be sure to include device ownership, support, and maintenance
• Set integration approach and employ standards-based technologies where possible
• Monitor and manage mobile devices and supporting infrastructure
Contact Information

Ilene Yarnoff  
Principal  
(o) 703/917-2574  
(e) yarnoff_ilene@bah.com

Brenda Ecken  
Principal  
(o) 571/346-5854  
(e) ecken_brenda@bah.com

www.boozallen.com