Security Implementation Considerations for Mobile and Wireless Technologies
NIST HIPAA Conference

May 12, 2010

This document is confidential and is intended solely for the use and information of the client to whom it is addressed.
Agenda

- Business Drivers
- Risks
- Security Implementation Considerations
As security professionals, we have been playing catch-up with trying to learn, analyze, and secure mobile and wireless technologies...

- **Capability drives adoption, the market will not wait for your organization to catch-up**
  - Initial adoption of BlackBerry empowered the mobile workforce, and the commoditization of mobility can expose your organization to data-security threats
  - With the rapid increase of mobile platforms, there are more endpoints than ever to secure and manage

- **Wireless devices will inevitably connect to your enterprise resources**
  - The balance between information protection and information access becomes more complex as the availability of mobile devices increases
  - Wireless transport occurs at the core, distribution, and access layers of government networks; it has become a standard feature that is embedded in many products

- **Influence wireless adoption, don’t react to it**
  - Wireless introduces complex security challenges from a planning, policy, technical, and implementation perspective
  - Enforce and influence the development of practical security standards and policies
  - A wireless breach can be equally damaging as a wired breach
Mobile devices extend the wired infrastructure, increasing the overall risk to our enterprise networks...
The concept of Mobility encompasses everything that touches voice and data that is not considered part of the wired architecture...

- Devices allow data to be **easily moved** and **accessed remotely**
  - Phones
  - PDAs
  - Memory cards
  - Consumer electronics

- This trend toward **“data in motion”** creates security risks to the enterprise
The adoption of mobile solutions mirrors the introduction of another key information technology 15 years ago – personal computers...

Mobile technology-based applications exhibit a similar adoption curve to PCs

- CIO enforces compliance with information resource management practices
- Develop enterprise-wide mobility capabilities
- Integrate into enterprise architecture; comply with security policies
- Rapidly adopted by pockets of users; “guerilla technology”
- Purchased from controllable budgets, not conforming to IT investment principles
- CIO exercises some limited control over adoption of the technology
- New technologies introduced by individuals to enhance mission performance
- First-generation often proprietary technologies; do not meet IT standards
- Use of technology is largely invisible to CIO

CIOs face substantial mission assurance risks – until mobile technology implementations are forced into compliance with IT architectures, policies, and practices
Mobile devices hold enormous potential to streamline and improve the delivery of healthcare...

- Mobile and wireless computing are advancing the entire health care industry in powerful ways
  - Asset tracking and management (RTLS)
  - Streamline processes
  - Reduce administrative redundancy
  - Decrease costs
  - Improve patient safety
  - Provides emergency access to EPHI

- Use of Handheld Mobile Devices growing rapidly
  - 30% of physicians access EPHI using a handheld device (31% are iPhone users) [source: SDI]

- Mobile computing solutions
  - Diagnostic
  - Treatment
  - Patient History
  - Billing
  - Reference
  - Drug Interactions
  - Referrals
  - Prescriptions
  - Patient Monitoring
  - Laboratory Services
  - Discharge Protocols
  - Communication with insurers, and much more…
Mobile and Wireless technologies offer key advantages over traditional telecommunications solutions...

<table>
<thead>
<tr>
<th>Mobile Attributes</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Always on (anytime)</td>
<td>Coordination and response</td>
</tr>
<tr>
<td>Portability (anywhere)</td>
<td>Data collection &amp; accuracy</td>
</tr>
<tr>
<td>Location-aware (geographic context)</td>
<td>Speed</td>
</tr>
<tr>
<td>Context-aware (volume and content)</td>
<td>Productivity</td>
</tr>
<tr>
<td>Reduction in operating costs</td>
<td>Real-time actionable information</td>
</tr>
<tr>
<td>Remote access</td>
<td>Continuity of operations</td>
</tr>
</tbody>
</table>

53% of organizations have at least 20% of their employees working remotely
- 2009 Yankee Group Study
A day in the life of a mobile worker...

6am – Checks e-mail from home via cable provider WLAN

7am – Files expense report from metro via wireless WAN

8am – Docks laptop at desk to print report for meeting

9:30am – Makes live demonstration at a meeting using laptop connected via office LAN

10:30am – Returns to desk and uses Bluetooth keyboard to input and send email

Noon – Collaborates on presentation during lunch via commercial Wi-Fi hotspot

1pm – Checks e-mail via wireless WAN in taxi en route to airport

2pm – Continues to work on email in airport via public Wi-Fi hotspot

2:30-4:30pm – Onboard airplane

5pm – Sends report via e-mail connected to hotel wired Internet connection
- Business Drivers
  - Risks
  - Security Implementation Considerations
Where is your organization today? Is your mobility operating out-of-band?

- 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
Mobile and wireless technologies introduce many new challenges for information security personnel…

- Personal devices vs. CDO issued
- 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
Users will rely on mobile and wireless technologies more and more to store and transmit sensitive data; consequently, the risk of data compromise escalates…

**Mobile Device Security Risks**

- Access to sensitive data stored on the device
- Access to data stored on corporate networks
- Malicious software entry point to enterprise network
- Ability to impersonate the authorized user

**Threats**

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

**Protection Needs**

**Enterprise Resources**
To successfully reduce risk to an acceptable level, your mobile and wireless initiatives should be fully integrated into your IT & IA Programs...

1. **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).

2. **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.

3. **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.

4. **Mobility Security Operations and Administration**
   - Enterprise mobile solutions are operated and administered according to defined requirements; security posture is periodically evaluated for compliance.
How bad is it really?

- 03 May – Laptops stolen from California health care organization
- 20 April – Health information contained on physician's stolen laptop
  - A laptop containing the demographic and health information of thousands of patients was stolen from a physician affiliated with the Massachusetts Eye and Ear Infirmary.
- 12 April – BitDefender Discovers PC Malware using iPhone as Bait
- 07 April – Sensitive laptops stolen from California hospital system
- Airport Insecurity (source: Dell and the Ponemon Institute, June 30, 2008)
  - Over 12,000 laptops and other devices lost in U.S. airports each week; only ~30% are reclaimed.
  - Over 50% of the laptops considered to contain sensitive data; ~35% take steps to protect or secure their laptop information
Are you ready for what’s coming next?

- **Near Field Communications**
  - Mobile payment
  - Electronic ticketing
  - Electronic keys

- **Femtocells**

- **Mobile Hotspots (Mi-Fi)**

- **Wireless USB**

- **Bluetooth low energy**

- **International Standards Bodies**
  - Internet Engineering Task Force
  - Payment Card Industry
  - IEEE
  - International Organization for Standardization
  - International Electrotechnical Commission

- **Domestic Standards Bodies**
  - National Institute of Standards and Technology / Information Technology Laboratory
  - American National Standards Institute
  - X9
  - International Committee IT Standards
- Business Drivers
- Risks
  - Security Implementation Considerations
The proper strategic imperatives to support a mobile and wireless ecosystem must be developed and thoroughly explored in the beginning…

**Standardization**
HW and SW standardization must be considered from start to reduce maintenance costs.

**Integration**
Integration is key to the effectiveness of system. Integration with back end systems must be evaluated.

**Security**

**Patient Safety**
Vital factor in driving the implementation of mobility in the health care field.

**Asset Management**
Hardware and user assessment must be regularly monitored to determine overall system effectiveness and to remove defective care delivery devices.
Extending enterprise security throughout your mobile ecosystem...

Technical Safeguards

- Implement technical policies, processes, procedures, and mechanisms for electronic information systems that maintain EPHI to allow access only to only those persons or software programs that have appropriate access rights
- Unique user identification, multi-factor authentication (AuthN) and role-based authorization (AuthZ) access controls
- Communications/session automatic logoff
- Confidentiality and Integrity of EPHI
- Audit Controls

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)
Mobile end points increasingly support and can leverage enterprise security protocols...
Secure mobility requires a balance of managerial, operational, and technical controls to secure and protect EPHI…
Mobile and wireless technology security implementation includes all components of the communications system...

People
- 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

End-point
- 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 & access
- Audit controls
- Remote wipe
- Data separation (personal versus sensitive)
- Automatic logoff

Communications
- Confidentiality Over the Air Transmission
- Authentication Of Devices
- Integrity Of Transmission

Perimeter
- Confidentiality (VPN)
- Device management
- Authentication Of Devices
- Authentication Of Users
- Identity Management
- Access Control To Network Services
- Enforcement of Enterprise Security Policy
- Audit and logging controls
- Provisioning
- Application management
- Intrusion detection

Enterprise
- Integrity Of Application Data
- Access Control To Data Bases and Applications
- Other application-specific security controls
- Access Control To Network Resources
- Access Control Related To Specific Content
- Audit and logging controls
Established security techniques can be leveraged to help mitigate risks to mobile devices...

<table>
<thead>
<tr>
<th>Mobile Device Security Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mobile device access</strong></td>
</tr>
<tr>
<td><strong>Power-on authentication</strong> – Require a power-on password or PIN, so the device cannot even be powered by an unauthorized user. Implement a standard process for creating unique user names and pins. Controls also applies to session timeouts requiring re-authentication to device to gain local access.</td>
</tr>
<tr>
<td><strong>Auto-lock</strong> – Configure device to automatically lock up after a certain period of time.</td>
</tr>
<tr>
<td><strong>Two-factor authentication</strong> – Implement two-factor authentication for access to systems that contain EPHI. Consider the use of tokens, call-back, and biometrics.</td>
</tr>
<tr>
<td><strong>Data storage</strong></td>
</tr>
<tr>
<td><strong>Data encryption</strong> – Establish data encryption for mobile devices. Identify the types of hardware and electronic media that must be tracked (hard drives, digital memory cards) and develop inventory control systems.</td>
</tr>
<tr>
<td><strong>Auto-run applications</strong> – Prevent memory cards from automatically running specific programs.</td>
</tr>
<tr>
<td><strong>Data erase and recovery</strong> – Ability to remotely wipe the remote end point and to conduct forensic analysis.</td>
</tr>
<tr>
<td><strong>Data transmission</strong></td>
</tr>
<tr>
<td><strong>Cryptography</strong> – Implement and mandate appropriately strong encryption solutions for transmission of EPHI. For example access can be implemented over SSL, IPSec or a similar VPN technology. Includes encryption, integrity, authentication, and non-repudiation controls.</td>
</tr>
<tr>
<td><strong>Data access</strong></td>
</tr>
<tr>
<td><strong>Role-based</strong> – Employ role-based access as part of a user-provisioning solution. Different users may require different levels of access based on job function. Develop and employ proper clearance procedures and verify training of workforce members prior to granting access. Access to enterprise resources should be role-based and monitored for abnormalities.</td>
</tr>
<tr>
<td><strong>Logging and Auditing</strong> – Implement logging and auditing on device and enterprise network. Ensure that the issue of unauthorized access of EPHI is appropriately addressed in the required sanction policy.</td>
</tr>
<tr>
<td><strong>Signed applications</strong> – Allow only signed applications to be loaded onto the devices. Signed applications should be checked during install and execution/runtime.</td>
</tr>
</tbody>
</table>
Security professionals should leverage NIST guidance and other industry best practices to establish baseline security requirements for mobile and wireless technologies...

<table>
<thead>
<tr>
<th>Category</th>
<th>NIST SP 800-53 Rev3 Control Name</th>
<th>Control No.</th>
<th>BlackBerry Enterprise Solution</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>
</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>
</tr>
<tr>
<td>Access Control</td>
<td>Concurrent Session Control</td>
<td>AC-10</td>
<td>Allow Split-pipe Connections</td>
<td>FALSE</td>
</tr>
<tr>
<td>System and Communication Protection</td>
<td>Public Key Infrastructure Certificates</td>
<td>SC-17</td>
<td>Certificate Status Cache Timeout</td>
<td>7 days or less</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.

Booz | Allen | Hamilton
Leveraging two-factor, token-based authentication for mobile identities…

1. Mobile Token is installed on end user's mobile device
2. User submits requests for enterprise service or resource
3. Organization responds with a OTP based on user credentials
4. User submits OTP to complete the two-factor authentication process

Managing mobile and user identities is a catalyst to extending enterprise services and resources to mobile users. The benefits of extending enterprise authentication services and resources will strengthen an organization's defense-in-depth posture.
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 – DRAFT Guide to Securing WiMAX Wireless Communications
  - IR 7497 - DRAFT 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.

---

Matt Sexton  
Senior Associate  
(0) 703/984-1452  
(c) 703/201-4483  
(e) Sexton_Matthew@bah.com