Mobile Device Security
NIST HIPAA Conference

May 19, 2009

Briefing summary

- Mobility Business Drivers
- Mobility Risks
- Secure Mobility and Best Practices

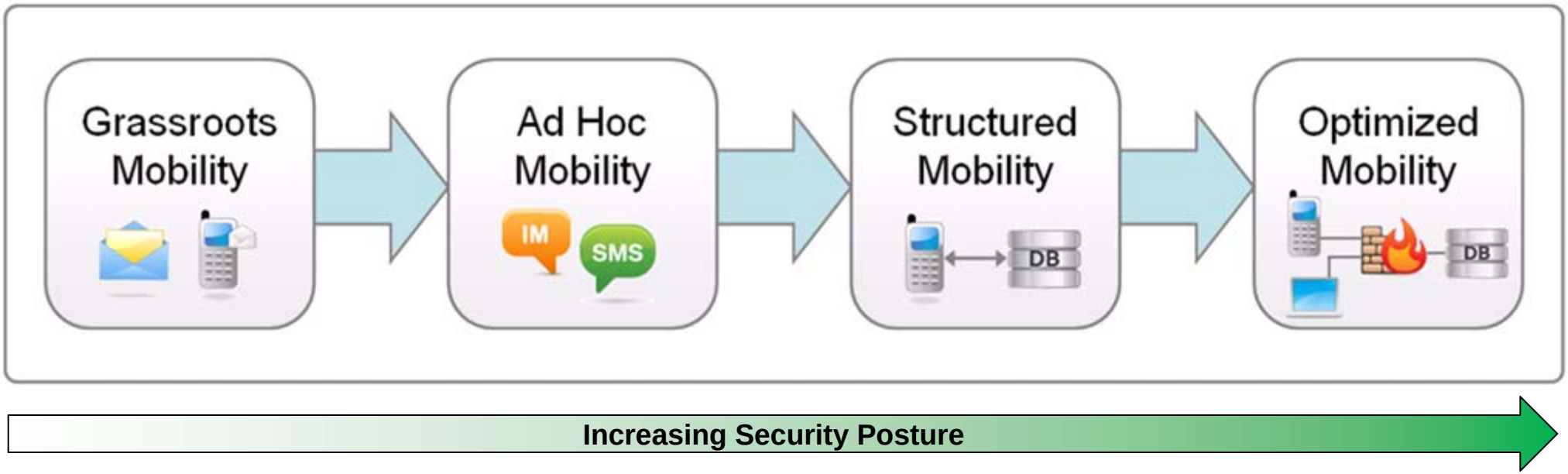
Mobile devices hold enormous potential to streamline and improve the delivery of healthcare

- **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 PHI
- **Use of Handheld Mobile Devices growing rapidly**
  - Estimated 60% of doctors will use handheld computers by 2007. (Harris Interactive Poll)

- **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…

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

Information technology will play a critical role in the delivery of healthcare, specifically the use of mobile-enabled business processes

- How it does business
- How it communicates with its patients and constituents
- How it delivers care
- The type of platforms and applications it deploys
- The type of talent it needs
- The support it requires
- The vendors it does business with
- How it protects the privacy and security of its information

Gartner Group's *Top 12 Actions for the Healthcare CIO, 2008* includes Action 2: "Mobilize" the Enterprise

- Mobility Business Drivers
- Mobility Risks
- Secure Mobility and Best Practices

Care delivery organizations have an ethical and regulatory responsibility to ensure the privacy and security of protected health information

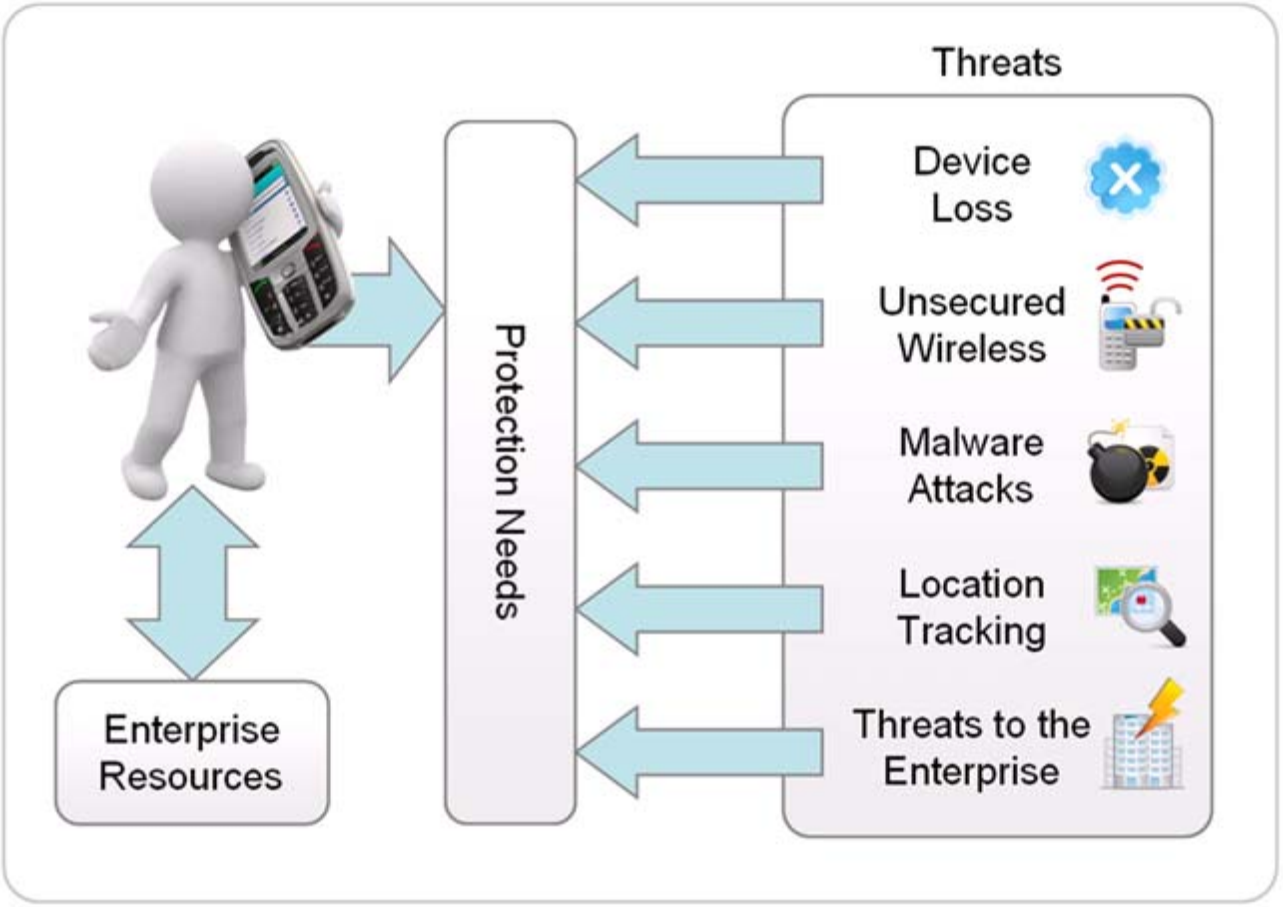
Key Facts and Findings

- The trend towards enhanced mobility is driven by both business demand and the end user
- Technology alone will not adequately protect PHI
- PHI security requires a comprehensive strategy that incorporates processes, people and technology
- The strategy must identify what needs to be protected, from whom, the likelihood of threats, and the security controls required to mitigate the inherit threats of mobility technologies
- Key elements to consider when approaching wireless security include areas where networks are most vulnerable, wireless technology's built-in security protocols, wireless and wired intrusion detection, and mobile device protection
- The delivery and implementation of Federal Privacy and Security requirements/guidance is not consistently communicated to private care organizations, e.g., physician practices

Mobile technologies enable many business processes and activities; however, these technologies also introduce new vulnerabilities and threats to the enterprise environment

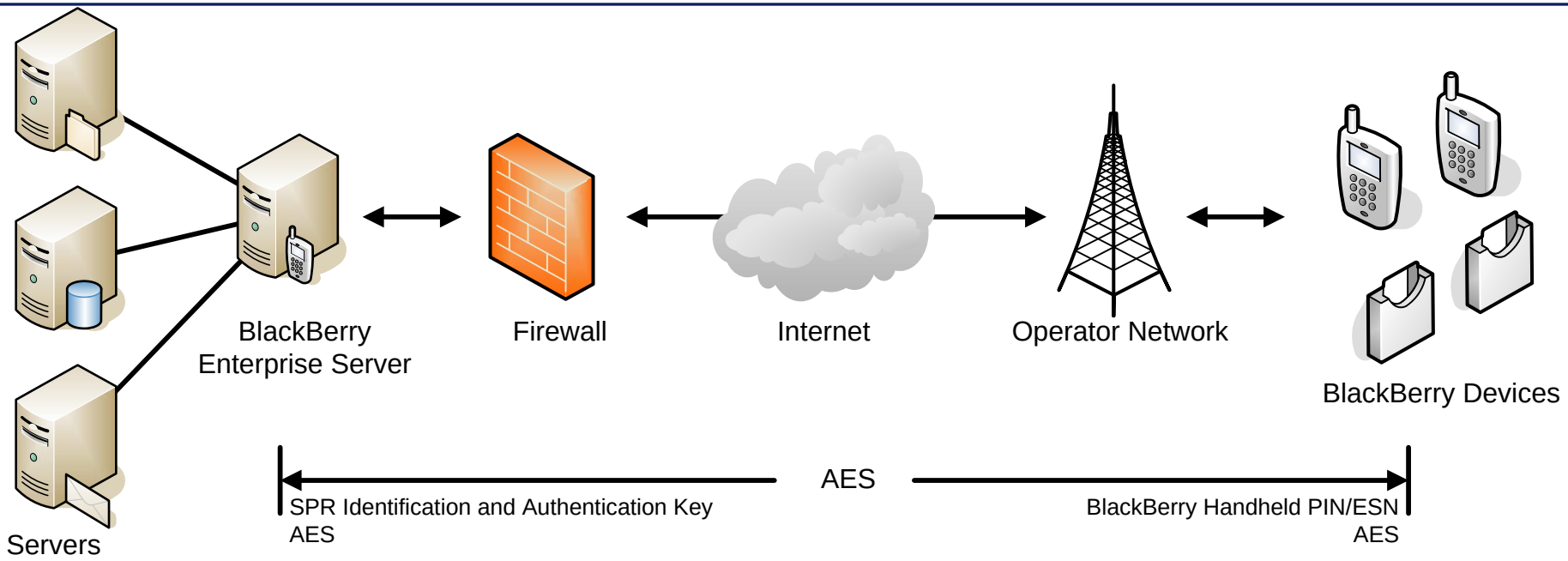
Mobile Device Security Risks

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



- Mobility Business Drivers
- Mobility Risks
- Secure Mobility and Best Practices

The BlackBerry Enterprise Solution is used by many Federal organizations as their “secure” messaging platform…



- BlackBerry Solution provides a centrally managed FIPS 140 validated end-to-end data-in-transit encryption solution
- The Federal government uses BlackBerry more than any other mobile messaging solution
- The BlackBerry Enterprise server solution disseminates security policy to an organizations BlackBerry devices to provide robust device setting control

BlackBerry Identification and Authentication

- User Authenticates to the device with a password/pin
- Device authenticates to the carrier network with its PIN/ESN
- Device authenticates to the BES with its PIN
- BES Authenticates to the MS Exchange Server
- S/MIME PKI Digital Signatures authenticate the email sender (when available)

BlackBerry security is dependant on properly implementing its control toolset

NIST SP 800-53 Rev2			BlackBerry Enterprise Solution		
Category	Control Name	Control No.	IT Policy	Recommended Setting	Comments
Access Control	Use of External Information Systems	AC-20	Allow Internal Connections	FALSE	Specifies whether applications, including third-party applications, can initiate internal connections (for example, to the BlackBerry MDS Connection Service)
System and Communications Protection	Mobile Code	SC-18	Allow Resetting of Idle Timer	FALSE	Permits third-party applications to reset the inactivity timeout value, bypassing the security timeout value
Access Control	Concurrent Session Control	AC-10	Allow Split-pipe Connections	FALSE	Specifies whether applications, including third-party, can open internal and external connections simultaneously
System and Communication Protection	Public Key Infrastructure Certificates	SC-17	Certificate Status Cache Timeout	7 days or less	Maximum number of days the device caches the certificate status

Conduct a NIST SP 800-53 Rev2 and BlackBerry Enterprise Solution IT Policy Controls crosswalk to determine and standardize IT Security posture.

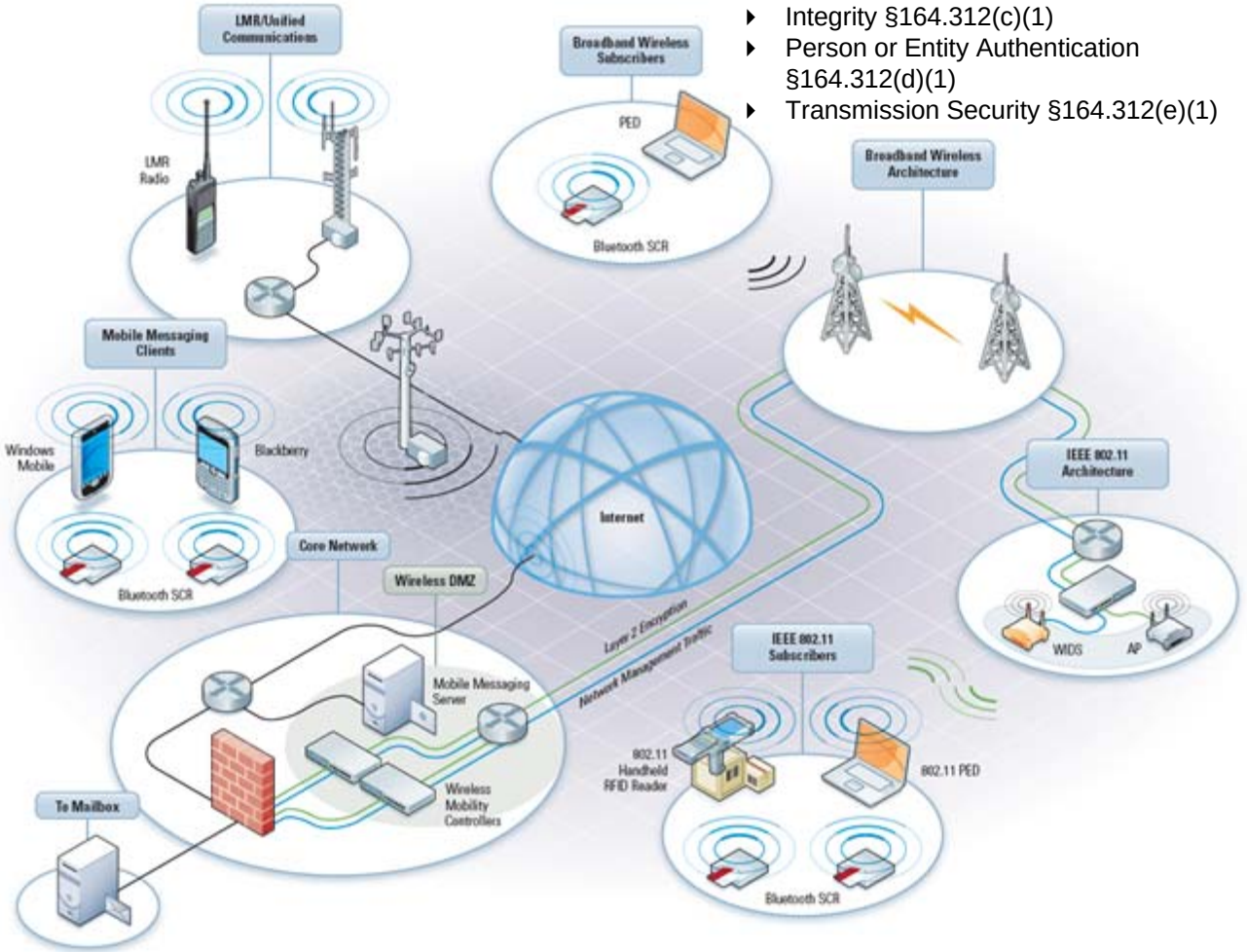
Extending enterprise security throughout your mobile ecosystem

Wireless Device Security

- 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

HIPAA Security Rule (Technical Standards)

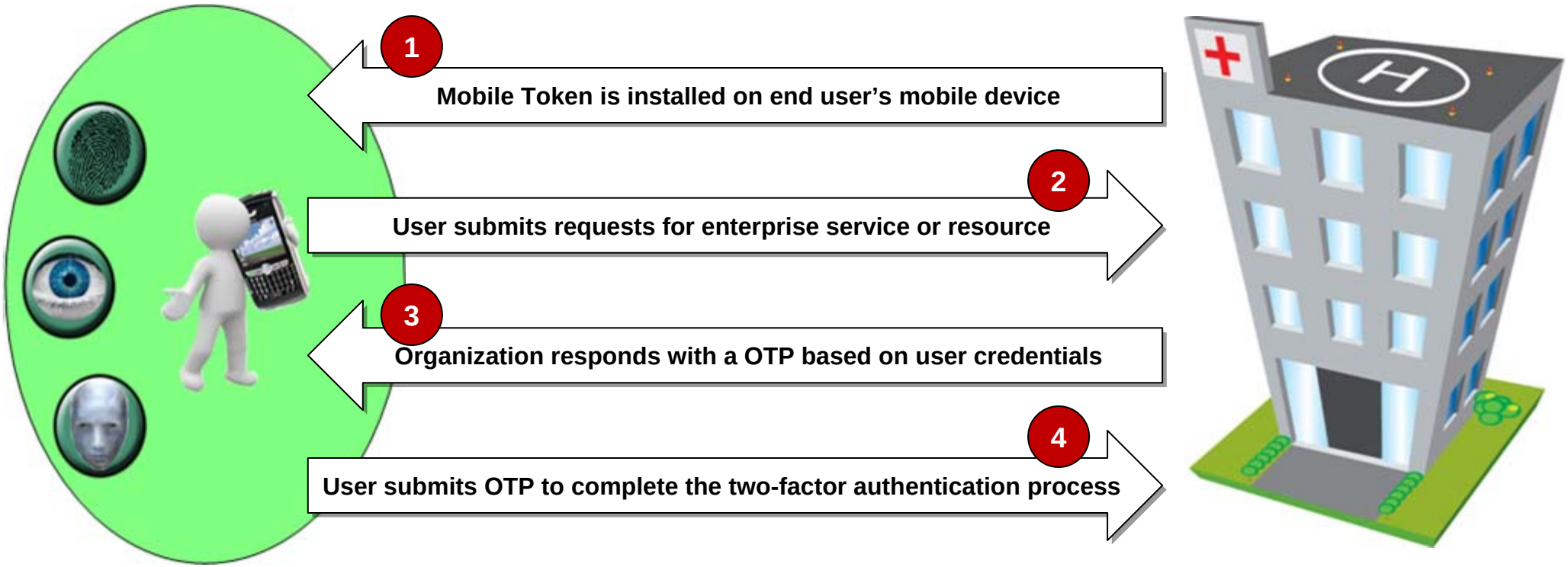
- Access Control §164.312(a)(1)
- Audit Controls §164.312(b)
- Integrity §164.312(c)(1)
- Person or Entity Authentication §164.312(d)(1)
- Transmission Security §164.312(e)(1)



Established security techniques can be leveraged to help mitigate risks to mobile devices

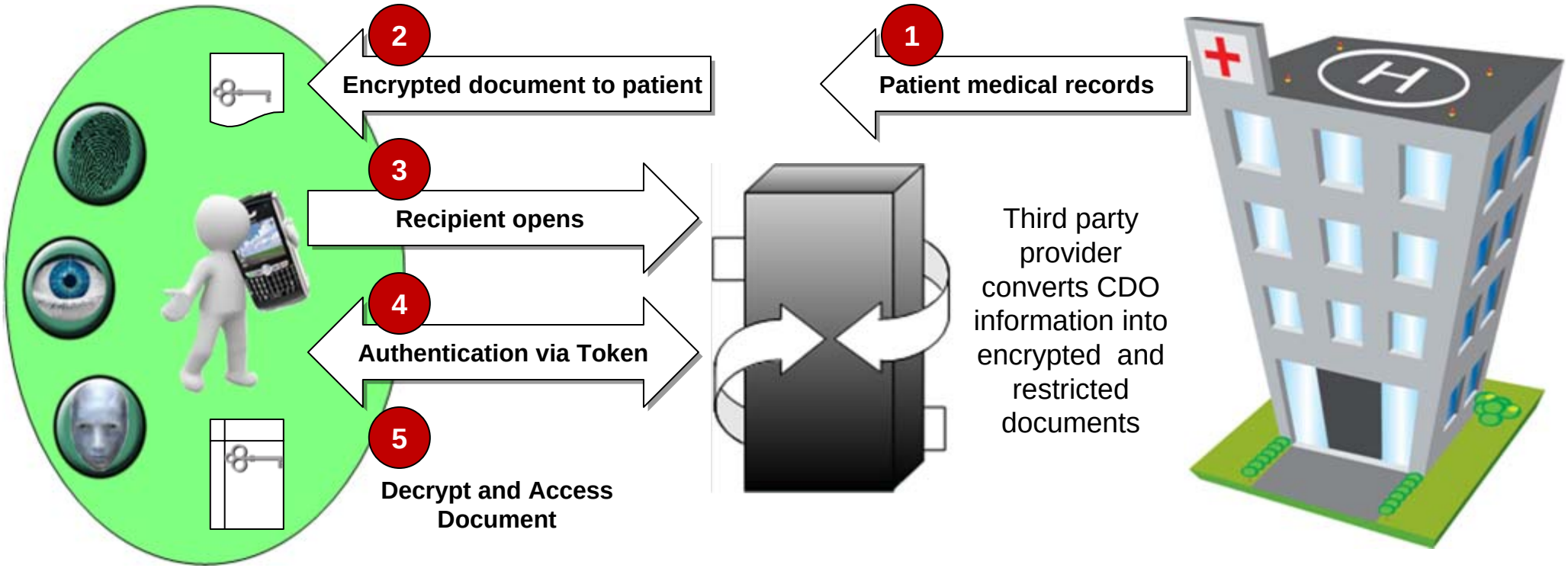
Mobile Device Security Recommendations	
Mobile device access	Power-on authentication – Require a power-on password or PIN, so the device cannot even be powered by an unauthorized user. Implement a standard process for creating unique user names and pins.
	Auto-lock – Configure device to automatically lock up after a certain period of time.
	Two-factor authentication – Implement two-factor authentication for access to systems that contain PHI. Consider the use of tokens, call-back, and biometrics.
Data storage	Data encryption – 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.
	Auto-run applications – Prevent memory cards from automatically running specific programs.
Data transmission	Encryption – Implement and mandate appropriately strong encryption solutions for transmission of PHI. For example access can be implemented over SSL, IPSec or a similar VPN technology.
	Signed applications – Allow only signed applications to be loaded onto the devices (S/MIME, Token-based).
Data access	Role-based – 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.
	Logging and Auditing – Implement logging and auditing on device and parent network. Ensure that the issue of unauthorized access of PHI is appropriately addressed in the required sanction policy.

Leveraging two-factor, token-based authentication for mobile identities



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.

Leveraging token-based authentication services for providing e-documents to mobile users



Multifactor authentication enables correspondence in a secure and efficient manner from health care providers.

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

Matt Sexton
Associate

Booz | Allen | Hamilton
strategy and technology consultants to the world

(o) 703/984-1452
(c) 703/201-4483
(e) Sexton_Matthew@bah.com

Backup Slides

Key Initiatives and Resources

- CMS has delegated authority to enforce the non-privacy provisions of the HIPAA Regulations, to include HIPAA Security. CMS has prepared guidance to provide HIPAA covered entities with general information on the risks and possible mitigation strategies for remote use of and access to Electronic Protected Health Information (EPHI).

- 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 (NIST), publishes its "Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule (SP 800-66 REV 1)".
  - 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 - DRAFT Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
  - IR 7497 - DRAFT Security Architecture Design Process for Health Information Exchanges (HIEs)