Mobile Security in Today's Healthcare Enterprise

Mobility and HIPAA

Today we will cover…

- 2013 HIPAA privacy and security changes
- A holistic approach to privacy and security
- Practical solutions for managing mobility in the enterprise

First let's review what's changed

Managing the environment has gotten even more complex…

- Significant changes to privacy, security and enforcement rules in 2013
  - Business Associate agreements
  - Breach notification
  - Privacy
  - Enforcement and penalties
- We are not a CISOs, but we need to be aware of the changes
  - Work with your CISO and compliance resources

Business Associates

- Expanded definition and requirements including contractors and subcontractors
- Increased penalties for negligence up to $1.5M
- BA definition is expanded to include entities who maintain PHI "On Behalf" of the Covered Entity
  - Examples: claims processors, analytics, utilization, e-prescribing
- If a vendor resource is primarily on-site need to decide if they are treated as BA or employee
- Transition of existing agreements must be completed by September 22, 2014
  - Qualify for grandfathering: Agreements prior to January 25, 2013 and not modified between March 26, 2013 and September 23, 2013.

Business Associates

Cloud computing services

- These organizations are potential BAs
- Example: Organizations that involve some type of data transmission
  - Do they access PHI on a routine basis?
  - Test: Access more than a random basis?
- Bottom line: work with compliance resources to review all potentials

Breach notification

- Strengthening and clarifications to HITECH breach notification requirements and rules
- Definition and more objective standards in assessing the probability that PHI was compromised
- Definition of more objective standards for when Covered Entities, BAs and subcontractors as to when a breach must be reported

Breach notification changes

- Risk assessment must consider these factors to determine probability of a breach
  - The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification
  - The unauthorized person who used the PHI to whom the disclosure was made
  - Whether the PHI was actually acquired or viewed
  - The extent to which the risk to the PHI has been mitigated

Breach notification changes

HHS has noted:

- "We have added language to the definition of breach to clarify that an impermissible use or disclosure of PHI is presumed to be a breach unless the CE or BA, as applicable, demonstrates that there is a low probability that the PHI has been compromised"
- In explaining why the "harm standard" was replaced: "We recognize that some persons may have interpreted the risk of harm standard in the interim final rule as setting a much higher threshold for breach notification than we intended to set. As a result, we have clarified our position that breach notification is necessary in all situations except those in which the covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised."

Breach notification changes

- Bottom line:
  - The unauthorized use or disclosure of PHI should be presumed a breach unless there is a "LOW" probability that the information was compromised
  - The new requirements lower the threshold for reportable breaches
  - All organizations (CE, BA, etc.) handling PHI must conduct a thorough and accurate risk assessment to clearly identify potential vulnerabilities and then implement a comprehensive risk management program (Corrective Action Plan)
  - Work with your compliance resources!

HIPAA Privacy Rule changes

- Many modifications including:
  - Notice of Privacy Practices (NPP)
  - Minimum Necessary Use and Disclosure
  - Copy of Electronic Health Information
  - Restriction on Disclosure to Health Plans
  - Sale of PHI
  - Research Authorization
  - Use of Genetics Information
  - Marketing
  - Fundraising
  - Disclosure of Child Immunization Proof to School
  - Decedents Disclosure of Information
- Work with your compliance resources!

HIPAA privacy rule changes

- Bottom line:
  - Changes & updates will require review and modifications in several areas of the enterprise
  - Individual rights have been expanded in significant ways. Patients can request their records in an electronic form
  - When individuals pay out of pocket in full they can instruct their provider not share any information about their treatment with their health plan
  - New limits on how information is used and disclosed for marketing and fundraising purposes including prohibiting the sale of health information without specific permission
  - Work with your compliance resources!

Penalties and enforcement changes

- Changes included:
  - Capped at $1.5M per violation, per calendar year
  - Implementation of a tiered civil penalty system required by HITECH
  - Penalties may be determined based on five factors
    - The nature and extent of the violation, including the number of impacted individuals
    - The nature and extent of the harm resulting from the violation
    - The history and extent of prior compliance
    - The financial condition of the covered entity or business associate
    - Such other matters as justice may require
  - HHS may waive penalties that are corrected within the 30-day cure period as long as they are not willful neglect
    - The counting of the 30-day cure period start when the entity knew or should have known of the violation
- Bottom line: HIPAA enforcement is now penalty based, not voluntary compliance

So what do we do?

Privacy and security in today's healthcare enterprise can be daunting…

- Managing systems…
  - Multiple EMR's
  - Shadow records
  - Medical devices
  - Diagnostic technologies
  - Modalities
  - HIE
  - Infrastructure
  - Public access
  - Mobility
  - BYOD
  - MORE!

So what do we do?

Threats come from all directions…

- Day to day operations.
  - Infrastructure attacks
  - Care delivery processes & communications
  - Business Associate interactions
  - Customer interactions
  - MORE!

So what do we do?

Programs are in place but are they taking a holistic approach?

- You have education but…
- You have monitoring but…
- You have risk analysis and auditing but…
- You have risk mitigation plans but…
- A mobility strategy will only work if it is built on a solid foundation

Components of a holistic approach

Successful privacy and security strategies are built on a multilayer holistic approaches including:

- Education
  - Beyond the rules
  - Should take place at all levels and all opportunities
- Risk analysis and auditing
  - Regularly scheduled assessments and auditing – round robin
  - Annual holistic assessment – All layers
  - Governance reporting – prioritize
- Risk mitigation
  - Can't do everything at once – doable and steady project cadence
    - Biggest bang for the work!
  - Governance – continually assess prioritization and subsequent planning

Components of a holistic approach

- Monitoring – Not just for techies, compliance and security resources
  - Infrastructure
  - Devices
  - Applications
  - Care delivery operations
  - More! - Ensure consistent approaches covering all layers of operations and technologies no matter where they take place
- Reporting/breach notification
  - Proactive plan – be ready if it happens
  - Scheduled exercise – similar to scenario based disaster planning

What is mobility?

Mobile devices are the fastest growing segment of technologies in the history of computers

- Growth rate is accelerating
- Convergence is on the horizon
- More than just laptops, phones and tablets
  - Anything that network enables: USB devices, cameras, iTouch, others

Mobility strategy

What are we facing?

- IBM Cyber Security report on the Threat Landscape
  - On average an organization will realize approximately 1,400 cyber attacks per week of some kind
  - Two of the most common are malicious code & sustained prob/scan
  - Approximately 80% of breaches are human factor based

Mobility strategy

Compliance mandates:

- HIPAA
- PCI DSS
- State regulations

Mobility strategy

- It's really not different…
  - Consistent with enterprise plan and approach
    - Education, Assessment, Monitoring, etc.
  - Entity must have sufficient controls in place
    - Allowed to place controls on the device – otherwise no connection
  - Can be costly – don't reinvent the wheel
    - Leverage industry tools
    - Fit within existing processes and resources

Mobile strategy

Specifically, mobility components need to cover:

- Education
  - Ensure management direction and support
  - Alignment with enterprise business & regulatory requirements
  - Raise awareness of the additional risks associated with mobile access
  - Clear goal: prevent unauthorized access, use & disclosure!
- Risk analysis and auditing – thorough enterprise assessment
  - Identify all mobile assets
  - Inventory all impacted polices, procedures & workflows
  - Include Business Associates

Mobile strategy

- Specific tactics to be considered
  - Registration of all mobile devices accessing the the enterprise
  - Determine device specific configurations – access security, apps, encryption, more!
  - Define specific standards for physical safeguards
  - Determine ongoing version and patch requirements and controls
  - Multilayered restrictions to information access
  - Encryption standards – transmission & storage <- Important!!
  - Malware protection – IOS, Android, Windows, etc
  - Backups – when and where are they needed
  - Remote disabling and wipe
  - Disposal - governance, policy and procedures

Mobility strategy

Mobility specifics to consider in employee agreements:

- Complete all required education and show proficiency
- Abide by all federal, state & local regulatory requirements
- Safeguard information
- Responsible for timely reporting of loss, theft, inappropriate disclosures and potential breaches
- Appropriate use of social networking
- Follow all license management & reconciliation policies/procedures
- Understand and be knowledgeable of the potential risks/penalties
- Device can be wiped – organization's or BYOD

Mobility strategy

Tools in the toolbox that can be leveraged

- Lets talk about virtualization
  - Are you moving towards a private cloud?
- Management – device & data (MDM)
  - Holistic approach - keep it simple
- Monitoring
  - Mobility specific
  - Leverage existing foundation

Mobility strategy

What about…

- Bring your own devices (BYOD)
  - Utilize same strategies or no access
- Custom "App" development
- Partners access
  - Strong BA
  - Limit access to minimum necessary
  - Ask questions - Do they really need to be administrators?
- Do you think about desktops and carts as mobile devices?
  - They can move so…

Action plan

Bottom "Bottom" line for 2013 changes:

- Work with your compliance resources to determine next steps for your organization
- Steps could include:
  - Changes to BA agreements should hold BAs directly liable for compliance
  - BAs should provide proof of completing comprehensive risk assessments, on a regular scheduled basis, and completion of the associated corrective action plans
  - Update breach notification and incident response policies, procedures processes and education
  - Conduct extensive risk analysis on a regularly scheduled basis
  - Execute a comprehensive corrective action plan

Action plan

- Ensure your activities take a holistic view
  - Education at all levels and in daily discussions
  - Risk analysis, auditing and prioritization
  - Monitoring – not just technology
  - Reporting and breach notification – test the plan!

Questions?

Thank you to

ecfirst