Out of Sight, Out of Mind: Working Offsite

Kate Borten, CISSP, CISM
President, The Marblehead Group

Key points

- Recognizing the full scope of responsibility
- CMS Security Guidance highlights
- Recommendations for administrative, physical, and technical controls

Historic attitude

- Focus on “production” systems and main data center
- Hard enough to secure, without looking beyond
- Sometimes policy banned removal of data, but management looked the other way since offsite work contributes to productivity

HIPAA got it right

- Security rule forces Covered Entities to acknowledge offsite work and manage it
- CEs are responsible for Protected Health Information wherever it is
- Workstation Use & Workstation Security standards explicitly require protections for all devices & media and surroundings

Full scope includes …

- Work via remote access (e.g., VPN) *and* stand-alone
- Accessing production systems (e.g., EHR) *and* email or other non-PHI systems
- Using CE-owned devices & media *and* personally-owned devices & media
- Use of public kiosks, wireless networks?

Offsite work and risk level

These are “givens”:

- Using PHI outside CE’s physical boundaries has higher risk than working inside
- Using portable devices and media for PHI access/storage has higher risk than fixed devices and media
- Using public kiosks and public wireless networks is very risky; they are untrusted

Vulnerabilities

- Vulnerabilities:
  - Portables with PHI (or providing access to PHI) easily lost and stolen, especially when traveling (commuting, working in the field, at hotels, etc.)
  - Offsite user surrounded by non-employees (family, strangers) not subject to CE policies, training, sanctions, etc., and not authorized for access to PHI
  - Logs, eavesdropping on public devices and networks

Threats and risks

(Threats exploit vulnerabilities, creating risks.)

- Threats
  - Mostly people: any conceivable human motivation from carelessness and curiosity to financial gain and malice
- Resulting risks to CIA:
  - Confidentiality – greatest risk: unauthorized disclosure of PHI
  - Integrity – less likely, but remote access to prod system could result in data modification
  - Availability - less likely, but remote access could introduce malware or bring system down

CMS Security Guidance

- Issued Dec 2006 following numerous incidents involving stolen laptops, etc.
- Download from http://www.cms.hhs.gov/SecurityStandard/
- Almost 2 years later and still seeing 1 or 2 per month (that make the news) healthcare breaches involving offsite portable devices & media

CMS Guidance groups PHI security risks

- Access to system – logon credentials lost/stolen or written down, failure to log off when leaving unattended
- Access to stored PHI (on home devices, portables, offsite backups) – device/media lost/stolen; residual data on home/public devices
- Transmission – eavesdropping on open networks (Internet, wireless)

Remedies: Policies & procedures – 1

- "Acceptable use," "clean desk" and similar policies ***on steroids*** such as
  - No sharing access; be aware of screen angle; don't leave device logged on and unattended
  - Log off; lock up papers & e-media; shred
- Consider providing equipment and banning use of personally-owned

Remedies: Policies & procedures – 2

- Device inventory
  - Include personally-owned
  - Identify uses
    - Breach notification: How to determine what records were breached
  - Be sure termination process includes checking inventory
    - Personally-owned devices: How to assure disposal of residual data

Remedies: Physical

- Home: Appropriate workspace (reserve right to inspect?)
- Locks: Portable devices and media (including paper) locked up when not in use or on one's person
  - Locked cases, locked drawers/file cabinets
  - At home, in hotels, while traveling
- Disposal - At home and on the road: Shred paper. Destroy e-media or use secure erasure.

Remedies: Technical

- End-user devices: AV s/w; personal firewalls; authentication; security patches
- 2-factor authentication for remote access
- Encryption
  - PHI stored on portable computers (e.g., laptops, PDAs, smart phones)
  - PHI stored on portable media (e.g., CDs, thumb drives, backup tapes)
  - PHI in transit over Internet and wireless

Training

- People are the weakest link
- But people can learn!
- Training on risks and the organization's specific behavior, physical and technical controls while working offsite is essential
- Sign agreement

Conclusions

- Yes, it's hard to manage offsite activities, and can cost money
- But that's where major risks lie
- And HIPAA requires it
- Implementation of new policies, physical and technical controls for offsite work may be the area of greatest change in healthcare security programs

Thank you!
Questions?

- Feel free to email or call me:

Kate Borten, CISSP, CISM
President, The Marblehead Group, Inc.
1 Martin Terrace, Marblehead, MA 01945
kborten@marbleheadgroup.com
www.marbleheadgroup.com
781-639-0532