2011 TECHNOLOGY CONFERENCE
Milwaukee • Sept. 14-15

IT Hardware Retirement Best Practices in Healthcare:

Regulations, Risks and Rewards

Neil Peters-Michaud

Cascade Asset Management

September 15, 2011

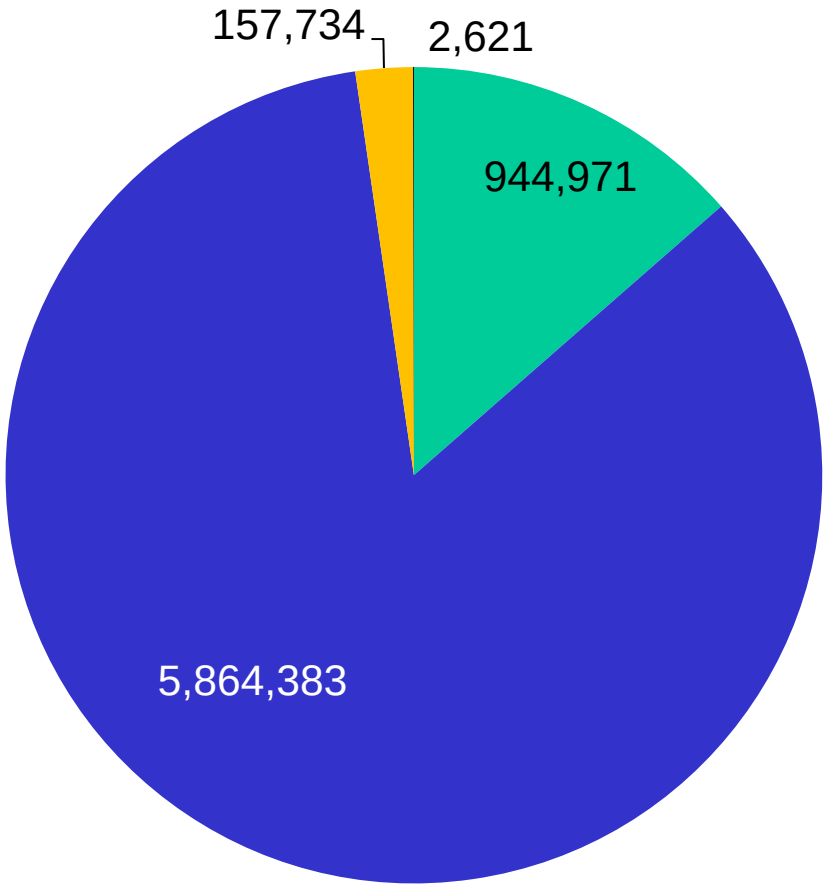
Do you Need to Deal with HIPAA Breaches?

Henry Ford Hospital	University of Nebraska Medical Center	Eisenhower Medical Center
Ochsner Health System	Grays Harbor Pediatrics, PLLC	Imaging Center of Garland
Indiana Regional Medical Center	Hanger Prosthetics & Orthotics, Inc.	Navos
Gary C. Spinks, DMD, PC	JEFFREY J. SMITH, MD	Troy Regional Medical Center
University Health Services, University of Massachusetts, Amherst	Osceola Medical Center	Union Security Insurance Company
Okla		tem
Univ		
Mountain Vista Medical Center	Saint Louis University	Tuba City Regional Health Care Corporation
Memorial Hospital of Gardena	Jefferson Center for Mental Health	New River Health Association
Zarzamora Family Dental Care	Ortho Montana, PSC	Reid Hospital & Health Care Services
Northridge Hospital Medical Center	Friendship Center Dental Office	Gene S. J. Liaw, MD. PS
Blue Cross and Blue Shield of Florida	New York City Health & Hospitals Corporation's North Bronx Healthcare Network	Medicare Fee-for-Service Program
Robert Wheatley, DDS, PC	Texas Health Arlington Memorial Hospital	Blue Cross and Blue Shield of Florida
Albert Einstein Healthcare Network	Lake Woods Nursing and Rehabilitation Center	Drs. Edalji & Komer
Clarksburg--Louis A. Johnson VA Medical Center	Accendo	Silverpop Systems, Inc. Health and Welfare Plan

In the last 12 months:

112 reported data breaches affecting over 6 million people.

Individuals Affected by Breaches on IT Hardware
(September, 2009 to July, 2011)



- Hacking/IT Incident
- Theft/Loss
- Unauthorized Access/Disclosure
- Unknown

64% of all breaches are a result of lost or compromised IT hardware (the remainder are from lost or compromised documents, emails, or improper disclosure of PHI.)

Source: US Department of Health & Human Services:
http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html

Key Points

1. Understanding compliance requirements and develop appropriate standards
2. Implementing policies and tools that best meet the standards
3. Making IT asset disposition a value added business service

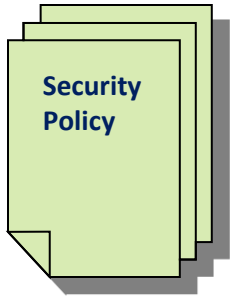
HIPAA Compliance Requirements *- some background*

- Health Information Portability and Accountability Act (HIPAA) of 1996
  - Defines Personal Health Information (PHI) and requires Covered Entities to **implement safeguards** to protect against unauthorized use of PHI
  - PHI is contained in physical documents, in communications (emails, mailings), on electronic media, on computing devices, on communication devices, in x-rays, etc.
  - Requirement to notify affected individuals and media of breaches
  - Penalties for failure to notify and for negligent activity
  - Business Associates (BA) who handle PHI for Covered Entities (CE) should be under contract and coordinate activities together.

HITECH Act 2009 ups the ante

- Health Information Technology for Economic and Clinical Health (HITECH) Act of 1996
  - Part of American Reinvestment and Recovery Act of 2009
  - $20 billion set aside to support electronic medical record implementation
  - Expands scope of who must comply with PHI protections
- Specific requirements introduced for PHI data “in disposal”
  - Data must be “unrecoverable” and “indecipherable”
- Business Associates are now potentially liable for breaches. Contracts must be in place between Covered Entities and Business Associates who handle PHI.

Compliance Requirements



- Covered Entities must have a designated "Security/HIPAA Compliance Officer"
- Need a security policy
- Appropriate Safeguards must be in place
  - IT must implement controls over network, communications, data in storage
  - There must be a way to track assets until PHI is destroyed on those assets

Security Policy Adoption

- Policy needs to be incorporated into other employee/corporate policies
  - Get buy-in across the organization
- Employees need to be trained, and training must be documented
  - Employees should sign off on corporate IT asset usage policies
  - Restrict use of personal devices for business
  - Discipline failure to follow rules
- Negligence when there is no follow-through on policies

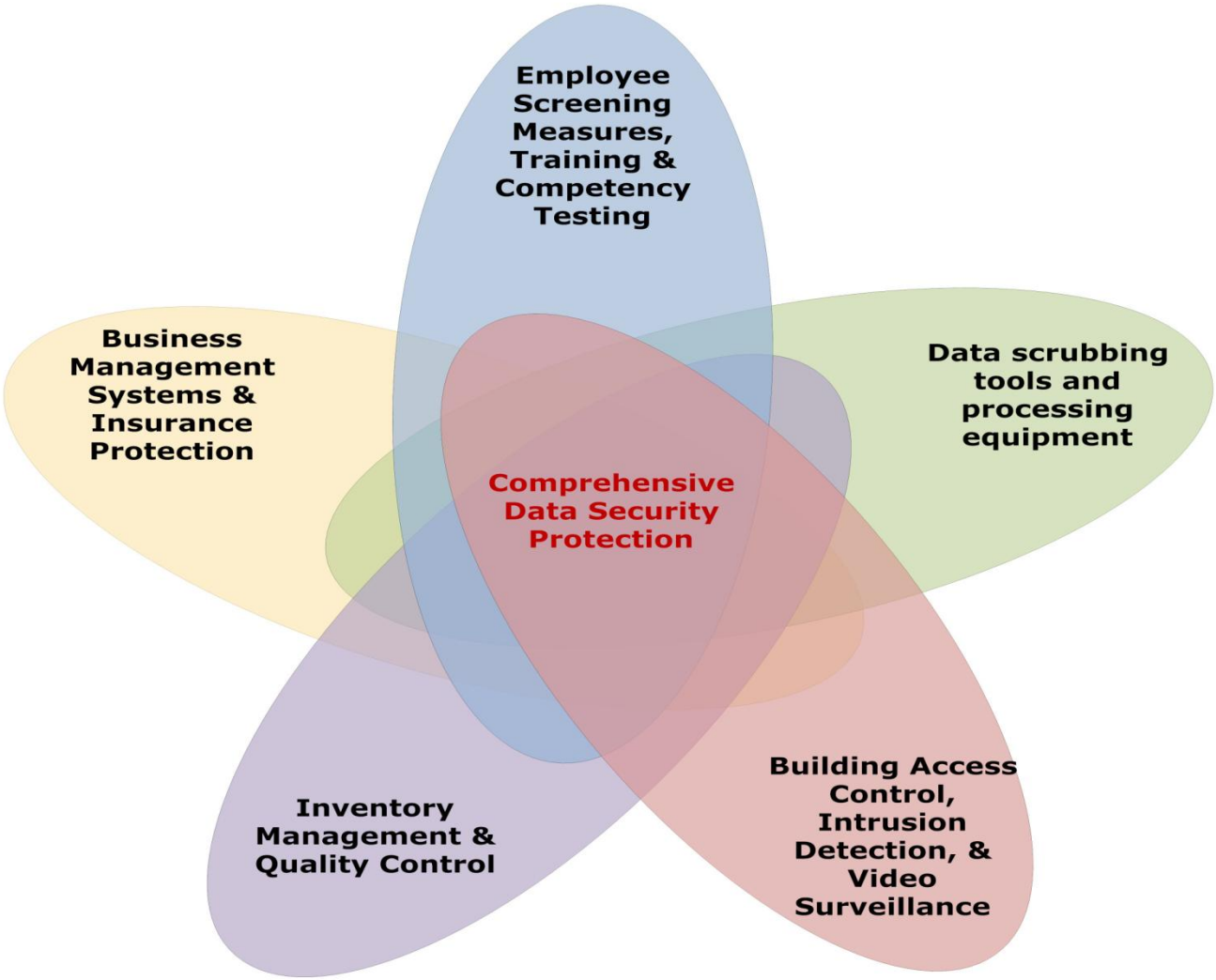
Training resources for you

Data Destruction Standards

- Guidance in HITECH is to follow NIST 800-88 "Guidelines for Media Sanitization"
  - Replaces the limited data wiping standard – Dept. of Defense 5220.22-M (3 pass wipe)
  - Comprehensive approach to secure data destruction on any storage device.
    - Hard drives, data tapes, cell phones, SSDs, storage in copiers/printers
  - Overwrite method must match company security requirement – 1 pass is often sufficient

Link to NIST 800-88: http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf

Effective Security exists in layers



Define Scope of Devices that may contain PHI











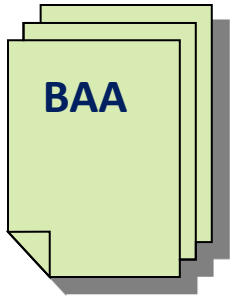

Track Devices – Asset Management

- Identify assets under your control
- Manage procurement, installation, changes, and disposal
- Storage of PHI on network/cloud vs. local devices
- Implementing encryption tools
- Restricting the use of difficult to control devices and personal devices

Mitigate risk of loss of hardware

- Most breaches from loss or theft of hardware
- Keep devices on the network and in communication with discovery tools
- When deciding to retire, keep hardware secure
  - Don’t let retired computers accumulate in a hallway
  - Don’t leave stacks of media or HDDs in the open
  - Do wipe drives or get equipment out to a responsible disposition vendor ASAP

Disposal of IT Assets



- Determine where PHI is destroyed
  - in-house or outsourced
- If outsource PHI destruction, a Business Associate Agreement (BAA) is required with vendor
  - Good idea to have a full contract in place to define limits of liability, insurance coverage (E&O) and service requirements
- BA must have safeguards in place
- BA must report suspected breaches to CE
- BA is potentially liable for breaches.
- Don't forget about damaged assets with PHI sent back for warranty return/replacement!

Transfer of assets (and responsibility) to 3rd party

- Only transfer title of assets based on detail of asset transfer
  - Need mutual agreement that specific items are being sent to disposal vendor
  - Inventory items on-site and get a sign-off of title transfer
  - Need to prove chain of custody
- Without detail on asset transfer, vendor can claim they never received an asset
- Doesn't matter if assets are owned or leased – still responsible for the data

Disposal – Agree to requirements

- Vendor should follow your data security standard
  - May require all items to be physically destroyed/recycled
  - If allow for electronic over-write and reuse of hard drives, need to define wipe standard
  - How can vendor ensure it follows process?
- Agreement on what happens if an asset or data is potentially lost
  - BAA will define response procedure
  - MSA will list insurance and indemnification coverage

Final disposition – closing the loop

- Vendor provides final disposition status for each asset
- Certificate of Destruction is a document from vendor that is their claim of how equipment was processed
  - Sometimes only as good as the paper they're written on – need clear details on individual assets
  - Good idea to audit these records
  - Expect timely reporting, otherwise there may be an issue
- Tie in final disposition report to asset management system
  - Provides cradle to grave accountability
  - Easiest access for audits

Why care about security during IT asset disposal?

Avoid Problems

- Keeps your CIO out of prison!
- Keeps your organization's name out of the paper due to breaches
- The cost to notify parties affected by breaches is ~ $115 per person.
  - In last 12 months, breach notifications cost healthcare organizations over $690 million
- Consider the organization's spend on other security programs as a benchmark for disposal investments
  - Estimate a cost of ~$25/system for complete and secure disposition

Make IT Asset Disposition a Business Value

- You are an essential part of the HIPAA security compliance program – get a seat at the table by offering solutions
- A third party disposition vendor transfers your liability and provides a good check on your system
- The faster data are destroyed, the better the organization's security is protected
- Institute an "employee recycling program" – to deal with security threats from institutional data on personal devices
- A quality IT asset disposition vendor will process your equipment in an environmentally responsible manner and promote sustainability goals – look for certifications from e-Stewards, R2, or others as a start, but have the environmental dept. complete their due diligence
- You could earn revenue from the resale of properly processed assets

pds 2011 TECHNOLOGY CONFERENCE
Milwaukee • Sept. 14-15

IT Hardware Retirement Best Practices in Healthcare:

Regulations, Risks and Rewards

Neil Peters-Michaud

Cascade Asset Management

Download documents following the Security Link on Cascade's homepage