

HIPAA Security Rule



IT Security Department
Information Technology & Computing Services
East Carolina University



Objectives

- Overview of HIPAA
- Overview of the HIPAA Security Rule
- Privacy versus Security
- Security Principles
- Basic Security Awareness Practices
- Email & Wireless Guidelines
- ePHI & Portable Devices
- Changes due to HITECH ACT
- Notification of Security Incidents
- Additional Information



What is HIPAA?

- Health Insurance Portability and Accountability Act of 1996
- National standard to bridge the gaps in the protection of patients' privacy and confidentiality
- All medical records and other individually identifiable health information used or disclosed by a covered entity in any form, whether electronically, on paper, or orally, are covered
- Two components: Privacy and Security



The Security Rule in a nutshell...

Legislation designed to:

- Ensure the confidentiality, integrity, and availability of all electronic Protected Health Information (ePHI) a covered entity creates, receives, maintains or transmits
- Protect against any reasonably anticipated threats or hazards to the security or integrity of the information
- Protect against any reasonably anticipated uses or disclosures not permitted by Privacy Rule



Privacy vs. Security

- **Privacy** = the right of an individual to keep his/her individual health information from being disclosed
- **Security** = the mechanism in place to control access to patient information, as well as to safeguard patient information from unauthorized disclosure, alteration, loss or destruction
- Unlike the Privacy Rule, the Security Rule affects only protected health information in *electronic format* (not oral or paper-based)

Security Rule Principles

- *Administrative Safeguards*
 - ✓ Policies and procedures designed to clearly show how the entity will comply with the act
- *Physical Safeguards*
 - ✓ Controlling physical access to protect against inappropriate access to protected data
- *Technical Safeguards*
 - ✓ Controlling access to computer systems and protecting communications containing PHI transmitted electronically from being intercepted by anyone other than the intended recipient



Food for Thought...

- Report Date: March 4, 2010
- Institution: Wake Forest University Baptist Medical Center
- A bag containing documents with the PHI of 554 patients was stolen Feb. 15 from an employee's locked car in the parking deck of an off-campus outpatient clinic. Hospital officials publicly revealed the theft on March 4.



Basic Security Awareness

- Incorporate secure practices into your everyday routine and encourage others to do the same
- Identify potential security incidents and be part of the solution
- Maintain an inventory of systems to know when a workstation, PDA, or laptop is missing
- Create written procedures or step-by-step instructions on how to perform a set of tasks
- Do not store ePHI on your workstation or portable devices
- Be cautious! Don't release information to unauthorized visitors or phone callers



Basic Security Awareness (con't)

- Use strong passwords and do not share them
- Lock your computer (Ctrl-Alt-Del) when not in use
- Guard your display from unauthorized eyes
- Don't install personal or unauthorized software
- Lock sensitive doors, drawers, cabinets
- Update anti-virus definitions - allow daily automated updates and scans



Food for Thought...

- Report Date: March 2, 2010
- Institution: The Open Door Clinic of Greater Elgin, IL
- The clinic stores patient information and medical history on a file-sharing network which is accessible to employees' personal laptops and home computers. A spreadsheet with information of about 260 of its patients was leaked as a result of the installation and use of file sharing software on computers containing patients' personally identifiable information.



Food for Thought...

- Report Date: December 16, 2009
- Institution: University of California, San Francisco
- Hackers may have had access to personal information for about 600 UCSF School of Medicine patients as a result of an Internet "phishing" scam. The security breach occurred when a faculty physician provided a user name and password in response to a scam e-mail message made to look as though it came from UCSF workers. Emails in the physician's account contained PHI, including Social Security numbers.



E-mail and Wireless Guidelines

- Email is not a secure method of communication. Do not send ePHI over email unless encrypted. Email messages can be intercepted by third parties or mistakenly sent to the wrong address.
- Do not access or send ePHI over a wireless network, unless the data is encrypted prior to transmission. Data sent over a wireless network can be captured by unauthorized persons in nearby buildings, parking lots, and streets.



ePHI and Portable Device Security

- Portable devices are NOT a secure platform for storage of ePHI. Any ePHI stored must be encrypted. It shall remain on the device only as long as necessary.
- Devices must have a power on password. Do not use the same password used to access ECU network resources.
- Turn off Bluetooth, Infrared, Wi-Fi and other wireless interfaces until they are needed. Bluetooth and Infrared shall be disabled while connected to the ECU network.
- Portable devices must be physically secured. Any loss, theft, or suspected unauthorized use of the device must be reported to the ECU Police immediately.



Food for Thought...

- Report Date: November 18, 2009
- Organization: Health Net (Shelton, CT)
- The personal information for almost half a million Connecticut residents could be at risk after a portable disk drive disappeared from Health Net six months ago. Health Net is a regional health plan.
- UPDATE(1/22/10): This case marked the first action by a state attorney general involving violations of HIPAA since the HITECH Act, which authorized state attorney generals to enforce HIPAA.



HITECH Act

- The **H**ealth **I**nformation **T**echnology for **E**conomic and **C**linical **H**ealth Act (HITECH Act or "The Act") is part of the American Recovery and Reinvestment Act of 2009 (ARRA).
- Because this legislation anticipates a massive expansion in the exchange of electronic protected health information (ePHI), the HITECH Act also widens the scope of privacy and security protections available under HIPAA



HITECH Act Implications

- New requirements around managing PHI includes extending accountability from healthcare providers to their business associates
- New federal rules for data breach notification, including specific notification thresholds, timelines and methods
- Increased and sometimes mandatory penalties with maximum fines ranging from \$25,000 to as much as \$1.5 million
- List of breaches on the HHS site:

<http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/postedbreaches.html>



Food for Thought...

- Report Date: January 14, 2010
- Organization: Blue Cross Blue Shield of Tennessee
- The theft of 57 hard drives from a training facility last October has put at risk the private information of approximately 500,000 customers in at least 32 states. The files contained customers' personal data and protected health information that was encoded but not encrypted. It is estimated that the Social Security numbers of approximately 220,000 customers may be at risk.

Notification of Security Incidents

- Report incidents to your direct supervisor immediately
- Contact the University Help Desk or open an incident ticket online:

252-328-9866 or <http://help.ecu.edu>



The Point of it All...

- The Administrative Medical Records and Billing Systems have security controls designed to protect ePHI. Use these systems as designed!
- No single security measure will provide total security.
- Security policies and procedures must be in place, taught, and enforced.
- Security is an ongoing process and we ALL have a role in securing ePHI.



Additional Information

- For questions regarding security policies or procedures, contact Paula Hutcherson, 328-9000 or hutchersonp@ecu.edu.
- Healthcare Applicable Use Policies
 - <http://www.ecu.edu/cs-dhs/hipaa/aup.cfm>
- Additional Computer Safety and Security Information
 - <http://www.ecu.edu/itsecurity/>



QUESTIONS?