

How ARRA HITECH Rule Affects Research

Research Compliance Conference
April 22, 2010
Joy Hardee, RHIA, CHRC, CHPS, CPHQ
Carole A. Klove, RN, JD, CHRC

1

Importance of HITECH Breach Notification requirements

- ▣ Health Information Technology for Economic and Clinical Health Act (HITECH) provisions of the American Recovery & Reinvestment Act of 2009 (ARRA)
- ▣ Effective date: 2009-2014

2

Breach Notification for Unsecured PHI: Interim Final Rule

- Issued 8/24/09
- Effective 9/23/09
- Penalties apply 2/22/2010
- <http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf>

3

Definitions

- "Breach" is defined as unauthorized acquisition, access, use or disclosure of protected health information (PHI) which compromises its security or privacy
- It is not a breach if:
 - The unauthorized recipient couldn't retain the data
 - Unintentional acquisition, access, or use of PHI by an employee or individual acting under the authority of a covered entity or business associate
 - Inadvertent disclosure of PHI from one person authorized to access PHI of a covered entity or business associate to another person authorized to access PHI at the covered entity or BA

4

Definitions

- ❑ "Unsecured PHI" is PHI that is not secured by a technology that renders the data unusable, unreadable or indecipherable
- ❑ HHS issued guidance identifying two methods for rendering PHI unusable, unreadable, or indecipherable:
 - Encryption
 - Destruction of data

5

Reality Check - What if your laptop or flashdrive was stolen?



6

Reality Check – Lost Laptop or Mobile Device

- ❑ Your laptop or flashdrive contained information about your current patients and study subjects. The device was locked in your trunk and it had a complex password on the device.



- ❑ Since you locked the laptop up and you had a complex password on the device, is this enough to keep you from being personally responsible for the loss of the patient information?



- ❑ What do you need to do if anything?

7

Risk Assessment

- ❑ Consider the type and amount of PHI involved in the impermissible use or disclosure,
- ❑ If the nature of the PHI does not pose a significant risk of financial, reputational, or other harm, then the violation is not a breach
- ❑ If type of services received (oncology, substance abuse, mental health, STDs) or if the PHI includes information that increases the risk of identity theft (social security number, account number, or mother's maiden name) then there is a higher likelihood that the impermissible use or disclosure compromised the security & privacy of the information.

8

Risk Assessment

- ❑ Covered entities and business associates must document their risk assessments, so that they can demonstrate, if necessary, that no breach notification was required following an impermissible use or disclosure of PHI
 - Make sure you have trained all workforce members on breach notification rules
 - Have a policy for privacy/security breaches
 - Have a procedure to follow for completing risk assessments
 - Set standards for use of encryption on portable devices and make sure your shredding company meets the applicable requirements (data destruction)
- ❑ Question to Consider: Are encryption standards and information security and privacy reviewed as a standard for each IRB or Protocol submission?

9

Determining a Breach or Not

- ❑ The covered entity or business associate must determine whether there has been an impermissible use or disclosure of PHI under the privacy rule
- ❑ The covered entity or business associate must determine, and document, whether the impermissible use or disclosure compromises the security or privacy of the PHI. This occurs when there is a significant risk of financial, reputational, or other harm to the individual
- ❑ The covered entity or business associate may need to determine whether the incident falls under one of the exceptions.

10

Breach Notification

- ❑ Individual notified within 60 calendar days of discovery of breach
- ❑ HHS notification (electronic format) > 500 immediately
 - HHS will post on their public website
- ❑ Media notification if > 500 individuals per state
- ❑ Log breaches < 500 and submit to HHS annually
- ❑ If contact information is unknown or outdated, by substitute notification:
 - Website or major media post if > 10 unknown
 - contact information via toll free number if questions
- ❑ Law enforcement delay is only exception
- ❑ IMPORTANT CONSIDERATION: Is the data loss also impacted by state laws and if so, which state laws are impacted?

11

Consider the Impact of HITECH Regulations and State Privacy Laws

❑ **Recent Headlines:**

“Kaiser patient medical records compromised”
 “Stolen external drive – workforce member fired”
 (Jan. 13, 2010, Victoria Colliver, San Francisco Chronicle Staff
 Writer)

“Connecticut Attorney General Sues Health Net
 Over Data Security Breach”

(Jan. 14th, 2010, IHealth Beat) (Lost Hard Drive)

12

Content of Notice Letter

- ❑ By first class mail to last known address
- ❑ Date of breach(s) and discovery
- ❑ Types of data at issue
- ❑ Steps individuals should take to protect themselves
- ❑ What the entity is doing to investigate, mitigate losses & protect against further breaches
- ❑ Contact information and Toll Free Number
- ❑ Consider adding a website link with FAQs relating to the breach and a media notification if needed

13

State Law Impact

- ❑ There are over 40 states with individual notification requirements for breaches also
- ❑ Have to follow state law and federal law requirements
- ❑ In NC we must notify individual without unreasonable delay, notify NC Attorney General's Office via their standardized electronic one page form at a minimum. Other requirements for substitute notice apply also with most state laws

14

Limited Data Sets

- ❑ A limited data set is created by removing the 16 direct identifiers listed in 164.512(e)(2) of the HIPAA privacy regulations. (Research, Public Health, HCO)
- ❑ The elements of dates, such as dates of birth, and zip codes are allowed to remain within the limited data set, which increase the potential for re-identification of the information.
- ❑ Because there is a risk of re-identification of the information within a limited data set, the Privacy Rule treats this as PHI that may only be used or disclosed as permitted by the Privacy Rule

15

Limited data sets

- ❑ The removal of the 16 identifiers in the limited data set presents a minimal risk of serious harm to the individual by limiting the possibility that the information could be used for an illicit purpose if breached.
- ❑ If the limited data set contains both DOB and zip code a risk assessment would need to be done to determine if the risk of re-identification poses a significant risk of harm to the individual.

16

Data Use Agreement

- ❑ A lot of research and public health activities rely on DOB and zip codes.
- ❑ Use and disclosures of limited data sets continue to be permissible under the Privacy Rule if the data use agreement is in place.

17

ARRA (HITECH Act) - Enforcement



ENFORCEMENT AND PENALTY CHANGES

- ❑ Criminal Penalties
 - Employees of covered entities and BAs are now liable for criminal and civil violations (42 U.S.C. Section 1320d-6).
 - Criminal offense – Obtain or disclose Individually Identified Health Information (IIHI) “knowingly” & “in violation of this part”
 - New definition: “A person shall be considered to have obtained or disclosed IIHI in violation of this part if the information is maintained by a covered entity and the individual obtained or disclosed such information without authorization.”
\$50,000/\$100,000/\$250,000 1/5/10 yrs in prison

18

ARRA (HITECH Act) - Enforcement

Civil Penalties

- **THEN (pre Feb. 17, 2009)**
 - \$100/violation to max. of \$25,000/yr
- **NOW (Feb. 18, 2009 on)**
 - 4 levels, with variable penalties, but with potential for up to \$50,000 per violation at each level (a 50,000% increase!)



19

ARRA (HITECH Act) - Enforcement

Violation Type	Each Violation	Not to exceed
Person did not know and with diligence would not know s/he violated law	\$100 to \$50,000	\$25,000 to \$1,500,000
Violation due to reasonable cause and not willful neglect	\$1,000 to \$50,000	\$100,000 to \$1,500,000
Violation due to willful neglect, but corrected in 30 days	\$10,000 to \$50,000	\$250,000 to \$1,500,000
Violation due to willful neglect and not corrected in 30 days	\$50,000	\$1,500,000

20

Research Protocols/IRB Forms

- ❑ Data Confidentiality and Subject privacy
- ❑ Describe how confidentiality will be maintained by providing details about the storage facility, device, duration of storage, data destruction method, and persons with access to the data (Note: encryption and destruction of data are the only 2 safe harbors that do not require a breach to be reported)
- ❑ DO NOT STORE RESEARCH DATA ON A PORTABLE DEVICE THAT IS NOT ENCRYPTED
- ❑ How will subject privacy be maintained during recruitment, data collection and data analysis?

21

How a Privacy Breach Can Happen

Here are a few of the ways a breach can occur:

- ❑ Information is mailed or faxed to the wrong patient, subject or physician or PI's office
- ❑ Laptops, computers, PDAs are lost or stolen and patient or research subject data is stored on the computer without security protections (e.g., encryption)
- ❑ Electronic systems are accessed where there is no business need to access the information (e.g., no waiver or IRB approval)
- ❑ Someone responds to an e-mail, which looks "official", where someone asks to verify their user name and password and it is provided. This is called "Phishing" and now someone has access to a computer system potentially with PHI and/or research data.

22

Case Studies for Discussion

- Things to consider as we review some case studies
 - Was there a breach? (Risk Assessment)
 - When did it occur and was there notice? (Create a timeline for notification)
 - Is so, was there PHI or IIHI on inappropriately accessed, used or disclosed? (PHI-IIHI Notification Template)
 - Was the device encrypted or email impacted? (Consider forensic analysis needs)
 - Are any other institutions impacted? Multi-centered study?
 - Who requires notification?
 - Patients/Subjects
 - State and/or Federal Agencies
 - Media
 - IRB or other Committee on Human Research
 - Study Sponsor
 - Do you need a call center to handle the calls or external mail service to send out the letters?

23

Questions and Discussion

24