

Reporting of HIPAA Privacy/Security Breaches

The Breach Notification Rule

**Protect
Patient
Information**



Objectives

- What is the HITECH Act?
- An overview-What is Protected Health Information (PHI) and can I protect patient's PHI?
- What do I need to know about the HITECH Act?
- What is a Breach (definition and examples)?

Objectives (cont.)

- Who Do I Call to Report a Breach?
- How Do I Report a Breach?
- What are the Breach notification Requirements?
- What are the Penalties of a Breach?

What is the Health Information Technology and Clinical Health Act (HITECH)?

- It is part of the ARRA (American Recovery Reinvestment Act of 2009) legislation that outlines the details of how PHI should be protected, and what to do if there is a Breach of PHI.

An Overview-What is Protected Health Information (PHI)?

PHI is:

- Information related to the patient and
- Information related to the patient's health care or payment

□ Examples:

- ❖ Patient's name
- ❖ Address
- ❖ Phone numbers
- ❖ Date of birth
- ❖ Social security number
- ❖ Medical record number
- ❖ Health diagnosis

How Can I Protect PHI?

- Only access PHI that is required for you to perform your job;
- Protect paper medical records from theft, misplacement, and access by unauthorized individuals;
- Only access/share the minimum necessary PHI required to perform your job;
- Take precautions when mailing, faxing, emailing, or transporting PHI so that such information does not go to unauthorized individuals;
- Take reasonable precautions when verbally sharing information so that unauthorized individuals cannot hear discussions of PHI;
- Where feasible, use encryption to protect stored or transmitted ePHI.

What Do I need to know about HITECH?

- Improves and expands current Federal Privacy and Security protections for health information
- The HIPAA Privacy and Security Rules *did not* change.
- The same rules apply to the protection of a patient's PHI.
- Imposes stiffer penalties for both individuals and health care facilities if these regulations are not followed.

Need to know about HITECH (cont.)

- Establishes notification requirements for the Breach of unsecured PHI.
 - (PHI that is unencrypted.)

What is a Breach?

- A breach of PHI is the unauthorized access, use, or disclosure of PHI that compromises the security or privacy of that information.

Breach Types:

- PHI from discarded paper documents, computer hard drives, flash drives, backup tapes and optical disks.
- PHI included in emails sent to the wrong recipient or PHI inappropriately attached to an email.
- PHI stolen and sold for monetary gain
- PHI obtained and disclosed by hackers
- PHI contained in lost or stolen paper documents, laptops, flash drives, backup tapes or optical disks.

Breach Types: (cont.)

- PHI that is disclosed due to the actions of a computer virus.
- PHI inappropriately posted or to which access is provided on a web server.

A **BREACH** can be Deliberate or Accidental

❖ *Here are some real life examples:*

- A Michigan-based health system accidentally posted the medical records of thousands of patients on the Internet (The Ann Arbor News, February 10, 1999).
- An employee of the Tampa, Florida, health department took a computer disk containing the names of 4,000 people who had tested positive for HIV, the virus that causes AIDS (USA Today, October 10, 1996).

Breach

Examples (cont.)

- A Nevada woman who purchased a used computer discovered that the computer still contained the prescription records of the customers of the pharmacy that had previously owned the computer. The pharmacy data base included names, addresses, social security numbers, and a list of all the medicines the customers had purchased. (The New York Times, April 4, 1997 and April 12, 1997).
- The health insurance claims forms of thousands of patients blew out of a truck on its way to a recycling center in East Hartford, Connecticut (The Hartford Courant, May 14, 1999).

What are Examples of a Breach?

- An appointment notice with a patient's name, diagnosis, and other identifying information, is sent to the wrong patient.
- A fax with patient demographic or medical information is sent to the wrong fax number outside of the hospital to someone who is not a treatment provider affiliated with the hospital.
- A medical record cannot be found after a due diligence search of the customary locations of the record.
- A portion of medical records is found in a public area such as a bathroom, the parking lot, etc.

Examples of a Breach (cont.)

- Someone, whose job function does not require that access, intentionally accesses a medical record, CLIQ, SMS, or other depository of patient information.
- A lap top or removable computer device (flash drive, floppy disc, CD, etc.) that contains PHI is lost or stolen.
- A trash bag with patient information is found in a public trash can.
- A health care provider is discussing a patient's medical condition using identifying information on a cell phone in a public area.

Important Things to Remember about Breaches....

- ❖ Breaches Happen!!
- ❖ You can report them anonymously
- ❖ All breaches must be reported
- ❖ **Anyone** who might be aware of an intentional breach must contact the Compliance Office at your facility.
- ❖ If you are unsure whether or not an incident is a breach, call the Compliance Office.

***WHEN IN DOUBT.....ALWAYS
CHECK IT OUT!***

Important Things...(cont.)

- ❖ Even the most careful employee may be involved in a situation that leads to a breach.
- ❖ Disclosures that are determined by the Privacy Officer to meet the definition of incidental disclosure are not reportable breaches.
- ❖ It is ***VITAL*** that any breach of PHI be reported **IMMEDIATELY** to the Privacy Officer.

Important Things...(cont.)

- ❖ Timely notification of any known Breach is **CRITICAL** as we only have 60 days from the discovery of the Breach to take the necessary action required by the Act.
- ❖ Each breach must be analyzed to determine if it should be reported to both the patient, as well as to the U.S. Department of Health and Human Services (DHHS).
- ❖ Not all breaches meet the definition of a reportable breach under HITECH.

Important Things...(cont.)

- ❖ For the purposes of complying with the HITECH reporting requirements, the Privacy Officer at LSUHSC-NO will do an analysis of each breach to determine if the facility must report the incident to DHHS.

Who Do I Call to Report a Breach?

- If anyone suspects or knows of any situation involving a Breach, you should report it immediately to:
 - The Privacy Officer at LSUHSC-NO
 - The Compliance Officer at LSUHSC-NO
 - The Office of Compliance Programs

How Do I Report a Breach?

❖ Contact the LSUHSC-N.O. Privacy Officer or the Office of Compliance Programs by:

➤ Telephone at:

- Office: (504) 568-2350
- Confidentiality reporting hotline:(504)568-2347, Or

➤ E-mail at: nocompliancehotline@lsuhsc.edu

Role of the Privacy Officer

- Responds to and analyzes each breach individually to determine if the facility must report the incident to DHHS.
- We have 60 days from the discovery of the breach to take the necessary action required by the Act.

What is LSUHSC-N.O. Required to Do if the Privacy Officer Determines a Breach is Reportable?

- Notify affected individuals within 60 days of becoming aware of the breach
- Provide in the notice to individuals, at a minimum, five specific categories of information
- Deliver the notice by first-class mail to each affected individual's last known address

Reporting (cont.)

- ❑ Notify major media outlets if breach involves 500 or more people (ex. Local newspapers, news)
- ❑ Notify HHS if breach involves 500 or more people
 - Posting on HHS website- *The secretary will make this information available to the public on their website*

Can I Lose my Job if I am involved in a Breach?

Yes. If the Privacy Officer determines that:

- There was a reckless disregard for the facility and LSUHSC-N.O. policies governing accessing, using, or disclosing PHI; and/or
- The improper acquisition, use, or disclosure of the PHI was intentional; and/or
- There is a proportionate, continuous trend of PHI being breached without improvement after corrective action has been taken.

What Are the Penalties?

- There is a tiered system for assessing the level and penalty of each violation:
 - **Tier A**-violations that are accidental not intentional-fines of **\$100** per violation up to **\$25,000** for violations of an identical type per calendar year
 - **Tier B**-violations due to reasonable cause and not willful neglect- fines of **\$1000** per violation up to **\$50,000** for violations of an identical type per calendar year

Penalties (cont.)

- **Tier C**-violations that the hospital corrected, but were due to willful neglect of the policies/procedures-fines **\$10,000** per violation up to **\$250,000** for violations of an identical type per calendar year
- **Tier D**-violations due to willful neglect that the hospital did not correct-fines **\$50,000** per violation up to **\$ 1.5 million** for violations of an identical type per calendar year

Additional Penalties

- Individuals and health care providers (hospitals, etc.) can also face civil and criminal prosecution, depending on the facts of the case.

THE END!!!

Please call us (Compliance) if you have any questions.....

➤ *Telephone at:*

- Office: (504) 568-2350
- Confidentiality reporting hotline:(504)568-2347, Or

➤ *E-mail at:* nocompliancehotline@lsuhsc.edu