North Big Horn Hospital District Privacy & Security Training

By Eileen Fink, RHIT, CHP Privacy Officer
Objective

This training will enable you to have a greater understanding of privacy and security compliance, how to recognize a concern, as well as give you the information you need in the event you must report a concern.
Agenda

- Important Definitions
- Patient Privacy - HIPAA/Omnibus Update
- Information Security
- Reporting a Concern
- Resources
- Take a Quiz!!
HIPAA (not HIPPA)

• Health Insurance Portability and Accountability Act – Regulations effective April 14, 2003
• Created standards for the exchange of electronic health care transactions
• Addresses the Security and Privacy of health data
HIPAA/HITECH Omnibus Final Rule

- Published in Federal Register – January 25, 2013
- Effective Date – March 26, 2013
- Compliance Date – September 23, 2013
• Protected Health Information—any information considered individually identifiable

• As an employee at North Big Horn Hospital, you have an obligation to protect patient privacy

• PHI includes: patient name, address, Social Security number, phone number, DOB, medical charts, verbal information, seeing patients at the hospital or clinic, etc.
Patient Privacy

- Accessing electronic patient information
- “Hallway” discussions
- Seeing friends/family at the facility
- Shredding
- Social Media/cell phones
Employee Access To Patient Info

- Patient information and medical records are of a confidential nature
- You are prohibited from viewing patient information that you do not have a bona-fide work related need to know
- Within the record, only review the minimum necessary information that you need for patient care
- You may not view your own record without first signing an authorization in the HIM department.
“Hallway” Discussions

• Example: Staff talking in the break room
• Any conversations regarding patient information should be done in a private location
• Consider the patient’s perception - Even if you never use a patient name
Friends/Family

• Example: Seeing your neighbor in the clinic waiting room

• If you see a friend or family member at the clinic or hospital, do not share with others

• Patients need to feel comfortable coming to North Big Horn Hospital for healthcare
Shredding

• Example: PHI accidentally thrown away and found at landfill or unlocked dumpster

• Anything with PHI must be shredded

• Shred containers should not look like garbage cans & should be emptied on a regular basis
How About Social Media Sites and Cell Phones/Cameras

Social Media Sites (Facebook, Twitter, etc.)
Remember that you are professionals, and the NBHH standards of behavior and HIPAA privacy also apply on Facebook and Twitter.

Cell Phones/Cameras – Note that there are specific policies regarding cell phone usage. Never send unauthorized texts containing patient/resident information to other staff members. Do not use cell phone cameras to take photographs of patients.

Remember - - Just because you don’t use a patient's name does not mean you are not breaching privacy. If someone else can determine who you are talking about it may be a violation.
HIPAA/Omnibus – Old vs New

CE (Covered Entity) = North Big Horn Hospital District

• OLD Rule

Marketing
• Marketing requires written authorization
• Certain communications about health-related products or services by covered entities to individuals not considered marketing
• Face to face marketing communications and promotional gifts of nominal value permitted without authorization

Fundraising
• CE permitted to use demographic information (includes insurance status) and dates of service to fundraise to individuals for its own benefit
• Each solicitation must describe how individual can opt out of future solicitations
• If individual opts out, CE must make reasonable efforts to honor opt out

• NEW Rule

Marketing
• Communications about health-related products and services by covered entity to individuals is now considered marketing and require authorization if paid for by third party
• Limited exception for refill reminders (and similar communications)
• Payment must be reasonably related to cost of communication
• Face to face marketing communications and promotional gifts of nominal value still permitted without authorization

Fundraising
• CE may also use department of service, treating physician, and outcome information to fundraise
• Each communication to individual must include “clear and conspicuous” opt out – no undue burden or more than nominal cost to exercise
• CE may not condition treatment or payment on individual’s decision
• CE must honor opt out (no further fundraising communications permitted)
• Flexibility provided in scope of opt out and method to opt back in permitted
More New Changes – Patient Rights

• **Right to Request Restrictions**
  - CE must agree to individual’s request to restrict disclosure of PHI to health plan if:
    - PHI pertains solely to health care for which individual has paid CE in full out of pocket
    - Disclosure is not required by other law
  - CE encouraged, but not required, to notify downstream providers of restriction

• **Electronic Access**
  - If individual requests electronic copy of PHI in designated record set, CE required to provide the e-copy to the extent it is readily producible
  - CEs permitted to charge reasonable, cost-based fee to cover providing the copy
  - CE must act on request within 30 days (60 days if PHI is not maintained or accessible to CE on-site)

• **Student Immunization Records**
  - CE may disclose proof of immunization of child to schools in States with school entry laws
  - Written authorization not required
  - Need prior oral or written agreement from parent or guardian
  - Must document agreement in patient’s record

• **Decedent Information**
  - Decedent’s information is no longer PHI after 50-year period
  - CE may disclose decedent’s PHI to family members and others who were involved in care/payment for care of decedent prior to death, unless inconsistent with prior expressed preference

• **Definition of Breach**
  - Impermissible use/disclosure of (unsecured) PHI is *presumed* to require patient notification, unless CE/BA can demonstrate low probability that PHI has been compromised based on a risk assessment of at least the following:
    - Nature & extent of PHI involved
    - Who received/accessed the information
    - Potential that PHI was actually acquired or viewed
    - Extent to which risk to the data has been mitigated
Enforcement

OLD RULE

- Willful neglect
  - OCR’s investigation of complaints/compliance reviews discretionary, regardless of nature of violation
  - OCR required to attempt to resolve indications of noncompliance by informal means

- Definition of Reasonable Cause
  - Circumstances that would make it unreasonable for the CE, despite the exercise of ordinary business care and prudence, to comply

NEW RULE

Willful neglect

- OCR will investigate or initiate compliance review whenever preliminary review indicates possible violation due to willful neglect
  - Makes discretionary the resolution by informal means, thereby enabling OCR to proceed immediately to penalties (such as in willful neglect cases)

- Definition of Reasonable Cause
  - Act or omission in which a CE knew, or by exercising reasonable diligence would have known, that the act or omission was a violation, but in which the CE did not act with willful neglect
  - Prevents a gap in penalty scheme
Protect Yourself and Your Patient’s Information

• Passwords
• Logging Off
• Access Audits
Passwords

• Example: Salt Lake City password sharing incident - Two hospital staff members were terminated when one used her friend’s password and emailed PHI outside of facility. Both the employee who shared her password and the one who used it were terminated.

• Each individual is given a unique username and is the only person that should use that sign-on

• Your password is essentially your electronic signature and must not be shared with anyone

• If you feel that your password has been compromised, contact the IS department immediately to have your password reset
Logging Off

• Example: Co-worker uses your logged-in computer to access patient information inappropriately

• Never leave a computer unattended with your logon still active

• Remember to log off or suspend your session each time you are done using
Access Audits

• Access audits are done to ensure patient privacy
• Each access report shows the username, name of patient accessed, date/time of access, and what information was being viewed
Patients Count On Us

• We’re all in this together

• Help your colleagues and coworkers maintain good quality HIPAA practices.
Reporting a Privacy Concern

• You are **obligated** to report any concerns or possible breach of PHI

• Compliance Officer or Privacy Officer
  – Eileen Fink (Privacy Officer): 548-5222
  – Kathy Walker (Compliance Officer): 548-5270

• Confidential Hotline: 548-5252

• Contact your department Manager or Supervisor
Privacy/Security Resources

- http://www.hhs.gov/hipaafaq/
- http://www.ahima.org/e-him/
- Eileen E. Fink, RHIT, CHP, Privacy Officer
Questions...if not, we are ready to take the quiz!