Terminology Check

- Business Associate – Business or individual who works with and performs functions for a Covered Entity that involves access of PHI. A Business Associate also is a subcontractor that creates, receives, maintains, or transmits PHI on behalf or another Business Associate.

- OCR - Office of Civil Rights, government branch that enforces HIPAA.

- Breach - An “acquisition, access, use, or disclosure” of unsecured PHI that is not otherwise permitted under HIPAA “which compromises the security or privacy” of the PHI.

As you know, HIPAA requires that we protect PHI by using...

- Administrative Safeguards
  - Written Policies and Procedures
  - HIPAA training

- Physical Safeguards
  - Locks on doors, windows, and/or file cabinets
  - Secure storage containers (i.e., safe)

- Technical Safeguards
  - Passwords, secure log-in, and time-outs
  - Encryption of PHI

(These are only a few examples, not an exhaustive list.)

But even with these tools in place, HIPAA violations continue and breaches still happen in many healthcare settings.

Let’s take a look now at some of the published reports on HIPAA violations and breaches that have occurred to learn from them.
HIPAA and Social Media sites are always a bad combination!

- Nurses used Facebook to provide shift change updates for their co-workers.
- No names were listed but enough details had to be included in order to prepare the next shift to take over the care of the patients.
- They were not authorized to do this but thought that since they did not give patient names it would be okay.
- It was not okay. While these disclosures were made with the best of intentions, they violated HIPAA because omitting a patient’s name does not guarantee that the person cannot be identified. The uniqueness of a situation alone could allow people to reasonably identify a patient.

Another example of Social Media horrors...

- A paramedic treated a sexual assault victim and posted information about the assault on his MySpace page.
- He did not disclose the victim’s name but he did post enough details that the news reporters were able to discover the identity of the victim and then searched for her at home.
- This resulted in a nightmare for the patient, the paramedic and the employer.

Facebook and MySpace - again!

- Nurses and staff members of an emergency room took pictures of a stabbing victim and posted them on Facebook. The breach of the patient’s privacy lead to the firing of 4 staff members and 3 others were disciplined.
- The photos were posted 2 days before they were reported to the hospital officials.
- Two workers in a hospital in New Mexico were fired from taking cell phone pictures of a patient receiving treatment and posting those images on MySpace.
- The photos were reported by an anonymous tip to the hospital supervisor.

This is why a policy on Social Media Participation is important to have!

- The purpose of a social media policy is to provide appropriate guidance for the workforce members when participating in the use of social media platforms and online technologies.
- It is not the intention of the policy to limit any workforce member from participation during their personal time; it is instead the purpose of this policy to establish acceptable use of, and the content of communications shared, within all social media platforms and online technologies.

Family Members and Friends

- You should never discuss any information in the reports you transcribe/edit with your family members and friends.
- Because you can be put in a difficult position if you work for a healthcare facility where they may seek treatment, or work for a company that does work for that facility, a policy for Special Exceptions to Workflow should be considered.
- The purpose of this policy is to provide guidance to the workforce for when they have inadvertently been assigned a report on family members, friends, or those individuals of special exception.
- Special exception individuals include those in an adversarial relationship (i.e. legal, personal, etc.), either currently or in the past.

From unintentional violations to intentional misuse of PHI.

- A 25-year-old LPN in Arkansas pleaded guilty for wrongful disclosure of PHI for personal gain and malicious harm in violation of HIPAA.
- She used her position as a nurse at a healthcare facility to access patient information that she disclosed to her husband, who subsequently called the patient and told the patient that he intended to use the information against him in “an upcoming legal proceeding.”
- The LPN was terminated by the healthcare facility and prosecuted for her actions.
  - She was sentenced to 2 years of probation with 100 hours of community service. It is uncertain if her nursing license will ever be reinstated by the state board.
Other examples of criminal intent.

- A Seattle phlebotomist at a cancer center stole PHI from patients’ health records including their credit card numbers.
  - He charged $9,000 to the credit card belonging to a patient with leukemia.
  - He was convicted and served 16 months in prison.
- Front desk coordinator for a large clinic in Florida stole the identity of approximately 1,130 patients which she sold to her cousin. He used the information for false Medicare claims.
  - She was sentenced to 6 months of home confinement, 3 years of probation, and ordered to pay $2.5 million in restitution.
  - Her cousin received 87 months in prison and also had to repay $2.5 million in restitution.

A recent case includes...

- A doctor in Los Angeles was sentenced to 4 months in prison for accessing and reading the medical records of his supervisor and of many high-profile celebrities.
  - He was also fined $2,000.
  - He accessed the UCLA record system 323 times during a 3-week period with having no legitimate reason.
  - He was terminated from his job.
  - He did not improperly use or attempt to sell any of the information that he illegally accessed.
  - He stated that he did not know that accessing the records was a federal crime.

Even a physician practice can be found in violation of HIPAA.

- The Phoenix Cardiac Surgery physician practice posted clinical and surgical appointments for its patients on an internet-based calendar that was accessible to the public.
  - When a patient complained to OCR, they investigated.
  - OCR found that the practice had inadequate HIPAA policies, limited safeguards to protect PHI, no security official, no security risk assessment, and had not performed HIPAA training.
  - They were fined $100,000 and have a corrective action plan in place to bring them into full compliance with HIPAA.

Disposing of PHI...duh!

- There are those cases where it is hard to decide if there is criminal intent or just people not using good judgment.
  - A medical billing company in Massachusetts obviously decided to skip the shredding process and instead put their old medical documents in a dumpster.
  - They were discovered by a Boston Globe reporter.
  - There were over 32,000 files found in the dumpster.
  - Fines and prosecution await the results of the ongoing investigation.

A recently published breach case involving medical transcription

- Hospital in NYC hired Professional Transcription Company who subcontracted work to a company called Bahoo.net to work on their account. Bahoo.net inadvertently made the patient information viewable through public internet search engines. Bahoo.net closed the website and destroyed the hard drive.
  - It was estimated that 37,000 records were exposed.
  - No financial information was disclosed (SS #).
  - Fines and prosecution await the results of the ongoing investigation.

Wall of Shame!

Health Data Breaches of more than 500 individuals

- More than 30,300,000 patients have been affected overall.
- Of the 879 total major breach events, an estimated 239 were caused by business associates.
- #1 reason for breach remains theft with over 450 cases reported.
- Laptops lead this list with nearly 200 reported cases.
- Portable electronic devices were involved in 110 breaches.
- #2 is unauthorized access/disclosure that accounts for over 170 cases.

Let's Dig a Little Deeper

- Covered Entities thefts that lead the list are:
  - Laptops 174 reported cases
  - Desktop computers 72 cases
  - Network server 16 cases
  - Other electronic devices 13 cases
  - Paper 78 cases
- Business Associates events that lead the list are:
  - Theft (not broken down by device) 86 cases
  - There is also the vague category called “loss”
  - Covered Entities had 62 cases of loss
  - Business Associates had 28 cases of loss

Unauthorized Access/Disclosure

- Covered entities had the following:
  - Paper 41 cases
  - Network Server 21 cases
  - “Other” 20 cases
  - Email 16 cases
  - Business Associates:
    - 41 cases (not specified)
Hacking/IT incident had the following:

- Covered entities:
  - Network Server 32 cases
- Business Associates:
  - 20 cases (not specified)

What if...

- You stored a couple of months of old reports on a USB jump drive. You are very careful about security so you always use encryption to secure your jump drive.
  - Today you realized that you have lost the jump drive.
  - You panic with the thought that you just caused a breach of hundreds of reports.
  - Is this a breach?

- You transposed the last 2 digits of a fax number and the report went to a nail salon instead of the patient’s referring physician.
  - Is this a breach?
  - What if the report instead went to a different physician?
  - Is that a breach?

What if...

- You selected the wrong doctor for the courtesy copy of the report you just finished.
  - Is that a breach?
What if...
• You selected the wrong patient name so that now the report you just finished is misidentified.
• Is that a problem?
• What happens when errors like these occur repeatedly?

Education is really the best method for avoiding HIPAA violations.

Examples of some common HIPAA violations:
• Inappropriate access and/or sharing of PHI with those who do not have a need to know.
  ▪ Snooping.
  ▪ Not logging off the system when you step away.
  ▪ Picking the wrong cc provider which causes a report to be shared with an unintended recipient.
  ▪ An error made in selecting the correct patient’s name for the report.

Have adequate protections for PHI.
• Do not throw PHI in the trash. Shred it.
• Do not post anything about any report on any social media sites.
• Do not send PHI in unprotected emails or text messages.
• Never share any information about any case with your family or friends.
• Only access patient information within the scope of your duties.
• Secure all media devices (i.e. jump drives, laptops, USB hard drives, etc.). Use encryption when available for protecting PHI.
• Limit the amount of PHI you store.

New England Medical Transcription thanks you for your attention to all HIPAA matters!

If you would like more information on this topic or on healthcare compliance issues, email me at bjthurley@aol.com
Or checkout my blog at http://brendajthurley.blogspot.com/

This presentation and its quiz have been preapproved by AHDI for 1 ML credit.