Introduction to Confidentiality and Privacy Under HIPAA

Overview:  What is HIPAA?

What is HIPAA and what does it govern?

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a multifaceted piece of legislation covering three areas:

- Insurance Portability
- Fraud Enforcement (Accountability)
- Administrative simplification (reduction in health care costs)

The first two components of HIPAA, portability and accountability, have been put into effect.

**Portability** ensures that individuals moving from one health plan to another will have continuity of coverage and will not be denied coverage under pre-existing condition clauses.

**Accountability** significantly increases the federal government’s fraud enforcement authority in many different areas.

The third component, **administrative simplification**, is arguably the most significant part of the legislation, and is the focus of this booklet.

Administrative simplification received little attention when the law was first enacted because its implementation date was later than the other two components. But today, two of its rules, privacy and security, are generating much discussion and debate in the health care community. The debate stems from the administrative, technical, and policy changes that the rules require health care organizations to make to protect their patient’s privacy and the confidentiality of protected health information (PHI).

HIPAA’s privacy and security regulations punish individuals or organizations that fail to keep patient information confidential. Until these regulations were enacted, there was no federal framework to protect patient information from being exploited for personal gain. Now, the Office for Civil Rights in the Department of Health and Human Services, has been charged with enforcing the HIPAA privacy rule.

**HIPAA** states that “covered entities” must comply with its regulations. Covered entities for HIPAA’s privacy and security regulations include most providers, clearinghouses and health plans.

Enforcement

Breaking HIPAA’s privacy or security rules can mean either a civil or a criminal sanction. Civil penalties are fines of up to $100 for each violation of a requirement per individual. For instance, if the hospital released 100 patient records, it could be fined $100 for each record, for a total of $10,000. $25,000 is the annual limit for violating each identical requirement.
Have you ever looked up a co-worker’s medical record to learn his or her birthday? Or read a neighbor’s medical history out of curiosity? Under HIPAA this could earn your organization a civil penalty and a fine.

Criminal penalties for “wrongful disclosure” can include not only large fines, but also jail time. The criminal penalties increase as the seriousness of the offense increases. For example, selling patient information is more serious than accidentally letting it be released, so it brings stiffer penalties.

“Egregious violations” such as the sale of a celebrity’s medical record information to a tabloid newspaper or the sale of health information to marketing or pharmaceutical companies for personal profit, could result in criminal penalties.

These penalties can be as high as fines of $250,000 or prison sentences of up to 10 years:

- Knowingly releasing patient information can result in a one-year jail sentence and $50,000 fine.
- Gaining access to health information under false pretences can result in a five year jail sentence and a $100,000 fine.
- Releasing patient information with harmful intent or selling the information can lead to a 10 year jail sentence and $250,000 fine.

Your facility is committed to protecting patient privacy and confidentiality. When you fail to protect patient information and patient records by not following your organization’s privacy policy, it can have an impact on your ability to do your job, your status with your organization, and your license to practice. You should carefully review your organization’s privacy policy and understand its requirements.

**Why are privacy and confidentiality important?**

Patient’s expectations of privacy and confidentiality are important to any hospital, physician practice, lab, nursing home, pharmacy, or other provider organization. Under HIPAA, the hope is that educated patients will be able to trust their providers and the organizations in which they work. To build trust, HIPAA calls on covered entities to learn the rules for privacy and confidentiality and then live by them.

Communications with or about patients involving patient health information should be private and limited to those who need the information for treatment, payment, and health care operations. Health care operations are activities such as conducting medical record reviews, training health care professionals and evaluating staff performance that don’t qualify as treatment or payment but are related to those functions and necessary for the organization operations. Only those with an authorized need to know will have access to the protected information. Hospitals and health care organizations have always upheld strict privacy and confidentiality policies. Unless you are new to healthcare, this will be familiar to you.
But there are changes. The U.S. government has strengthened the laws protecting privacy and confidentiality in response to instances of private medical information getting into the wrong hands.

**Protecting Privacy**

**The Privacy Regulation**

The privacy component of HIPAA protects individually identifiable health information that is transmitted or maintained in any form by covered entities. The regulations were published in the *Federal Register* on December 28, 2000.

Individually identifiable information is any information, including demographic information that identifies an individual and meets any of the following criteria:

- Is created or received by a health care provider, health plan, employer or health care clearinghouse
- Relates to the past, present, future physical or mental health or condition of an individual
- Describes the past, present, or future payment for the provision of health care to an individual.

It is important to note that HIPAA's privacy regulation is not limited to health information maintained or transmitted electronically, but covers information on paper or spoken.

**Confidential Information**

**What makes information identifiable?**

Any information that might identify someone is call individually identifiable information under HIPAA. Elements that made information individually identifiable include the following:

- Names
- Addresses
- Employers
- Relatives names
- Dates of Birth
- Telephone and fax numbers
- E mail addresses
- Social Security Numbers
- Medical Record Numbers
- Member or account numbers
- Certificate numbers
- Voiceprints
- Fingerprints
- Photos
- Codes
- Any other characteristics, such as occupation, which may identify the individual
Essentially, individually identifiable information is anything that can be used to identify a patient. Releasing any of this information for other than permissible purposes is a violation of the HIPAA privacy regulation.

Ways to Protect Confidentiality

The Minimum Necessary Standard

Health care workers must make a reasonable effort to disclose or use only the minimum necessary amount of protected health information they need to do their jobs.

Making minimum necessary determinations is a balancing act. Providers must weigh the need to protect patient’s privacy against their reasonable ability to limit the information that is disclosed and deliver quality care.

Before looking at patient information staff should ask themselves, “Do I need to know this to do my job?”

However, there is no minimum necessary requirement when it comes to treatment. Clinical staff is allowed to look at their patient’s entire record and share information freely with other clinicians directly caring for that patient.

There will also be occasions when you will have access to confidential information that you don’t need for your work.

For example, if a patient is placed in an isolation room, you may become aware of why he or she is there, or may suspect you know why. This is confidential information about a patient; do not communicate it to anyone else.

You may also see patient information on whiteboards throughout the facility. They are usually posted where the public cannot see them. In the course of providing patient care, you may work in areas where they are visible.

You must keep this information confidential. Do not disclose it to anyone, including coworkers, other patient, patient visitors, or anyone else who may ask.

In the course of doing your job, you may also find that patients speak to you about their condition. Although there is nothing wrong with this, you must remember that they trust you to keep what they tell you confidential. Do not pass it on.

Maintaining Records

When patient information is in your possession, you are responsible for safeguarding it. Do not leave it unattended in an area where others can see it. This is especially important in public buildings, provider locations, and areas with heavy pedestrian traffic.

When you are finished using paper patient information, return it to its appropriate location, i.e., the medical records department or a file at a
nursing station. When you are finished looking at electronic information, log off the system. Do not leave the information visible on an unattended computer monitor.

When discarding paper patient information, make sure the information is shredded or locked in a secure bin to be destroyed later. Leaving paper patient information intact in a wastebasket could lead to a privacy breach. The wastebasket could get knocked over. The paper information could fall off a recycle truck and blow down the street.

Computer equipment must undergo special processing to remove all traces of patient information before being thrown away.

Protecting Electronic Information

Ways to Protect Electronic Data

If you have access to electronic medical records, here are some ways to protect patient privacy:

- Use screen savers to block patient information displayed on unattended computer monitors
- Log off the system before you walk away
- Point computer monitors so that visitors or people walking by cannot view information.

Passwords

- Do not keep your password written down.
- Never share passwords with anyone.
- Avoid guessable names for your passwords, such as your last name or the name of your child.
- Change your password regularly according to your facility’s policy.

Faxes:

HIPAA does not address faxing patient information specifically, but it protects it under the privacy rule. Keep in mind that faxed patient information can easily fall into the wrong hands, which would be a violation of privacy. Before faxing any patient information, check with your supervisor to see if your facility has a policy that limits its use.

If you do fax patient information, make sure that you are faxing to a dedicated fax machine in a secure location and make certain that the person the information is being faxed to actually receive the fax. If you know you will receive a fax that contains patient information, tell the person faxing the information to warn you ahead of time so that you can be present to receive it.

Do not let faxed patient information lie around a fax machine unattended. Immediately dispose of or file faxed information before others can see it.
Helpful Hints to Use When Working with Computers:
• Review your organization’s policies on using computers
• Never share or open attached files from an unknown source
• Never send confidential patient information in an e-mail unless your facility has a policy that allows it and mechanisms in place to protect the information.
• Always double check the address line of an email before you send it.
• Never share your password or log on to the system under some else’s password.
• Always keep computer screens pointed away from the public.

Exceptions to the Rule:
There are exceptional cases in which providers are required to release patient information regardless of whether the patient agrees, and the law allows that.

The following list gives the circumstances in which an organization may release information:

• There are laws that require providers to report certain communicable diseases to state health agencies. The provider must report when patients have these diseases, even if the patient doesn’t want the information reported.
• The Food and Drug Administration requires providers to report certain information about medical devices that break or malfunction.
• Some states require physicians and other caregivers who suspect child abuse or domestic violence to report it to the police.
• Police have the right to request certain information about patients when conducting a criminal investigation.
• Certain courts have the right, in some case, to order providers to release patient information.
• Providers must report cases of suspicious deaths or certain injuries, such as gunshot wounds.
• Providers report information about patient’s deaths to coroners and funeral directors.

Adopted: 5/6/06
HIPAA and Privacy

Providing patients with quality healthcare includes protecting their confidential information. Our patients expect us to protect their information. If they do not feel they can reveal all of their problems to us, then we cannot provide the level of care that they need and deserve. Therefore, we must treat each patient’s information as though it were our own. HIPAA again provides us with the opportunity to demonstrate to our patients that they have not misplaced this trust.

What is covered:

- **Protected Health Information (PHI)** defined as:
  - Any oral, written or electronic information that is created or received by a healthcare provider that relates to the past, present or future physical or mental health of a patient
  - IDENTIFIES the patient

Things NOT to Do:

- Discuss patients where others can hear (hallways, cafeteria, elevators, etc.)
- Discuss patients outside the hospital with friends, family or others who do not have right to the patient’s information
- Remove original or copies of patient records from the hospital
- Discard PHI without destroying it
- Discuss PHI on cell phones or in non-BHS email
- Posting patient schedules for all to see
- Attempt to access PHI for which you have NO authority or need to see

Things TO Do:

- Place charts/papers backwards in wall pockets
- Protect computer monitors from casual viewing
- Save “triage” questions for private areas
- Make privacy and security a routine part of your day
- Place all PHI in proper bins for destruction
- Confirm the identity of anyone asking for information; confirm their authority to have the information
- Provide ONLY the minimum amount of PHI necessary for the intended purpose
- Convey to the patient in every way possible that his/her privacy is important

Sanctions:

- 45 CFR 164.530 (f) requires entities to have and apply appropriate sanctions
- Sanctions must also be documented:
  1. Counseling
  2. Probation/Final Warning
  3. Termination
Federal Privacy Rule Penalties:

- Holds violators accountable, with civil and criminal penalties, if they violate patient’s privacy rights
- Civil penalties for HIPAA violations
  - $50,000 - $250,000 in fines
- Criminal penalties for HIPAA violations
  - Imprisonment from 1 – 10 years

How to File Privacy Complaint:

- Contact Privacy Coordinator: Greg Bianca
  - Extension: 5040
    - Medical Records – BMC
- Complete Privacy Complaint Form (available on Speech Docs)
- Patients also have the right to directly contact the Office of Civil Rights

Adopted 5/6/06