Health Insurance Portability and Accountability Act (HIPAA) Education

Privacy for Beginners: What Every Healthcare Worker Needs to Know About HIPAA and Privacy

HIPAA and Privacy Introduction

Maintaining patient privacy has always been of critical importance at Sound Diagnostics of Northwest Florida. It is a responsibility of every employee. The **H**ealth **I**nsurance **P**ortability and **A**ccountability **A**ct (HIPAA) establishes new requirements for the handling, processing and storage of patient's health information. These new regulations **do not replace existing confidentiality policies** but further support and strengthen the commitment to keep patient information secure. Everyone involved in healthcare must be trained on these new requirements. This training session will try and put into words and examples the basic requirements of HIPAA and its Privacy Rules. You will be receiving additional information and training as part of Sound Diagnostics of Northwest Florida's ongoing compliance training.

HIPAA and its Rules

There are three different sets of regulations included in HIPAA:
1. Privacy Rules – Effective 4/14/03.
2. Standard Transactions – Effective 10/16/03.
3. Security rules – Effective 4/21/05

The Privacy Rules affect every healthcare worker, volunteer and physician no matter where they work in the healthcare delivery system by identifying certain patient information as "Protected Health Information" (PHI). PHI means any information, whether oral or recorded in any form, that is created or received by a health care provider and relates to a past, present or future medical condition or payment for services of an individual. The Privacy Rules give us guidance on how, when and with whom PHI can be shared.

Key Principles of the Privacy Rule

Consumer Control

Patients have a right to see their own medical records and to REQUEST changes to the records. Providers do not have to honor the request but must document the request and the reason for denial. Patients can request a listing where a provider has sent their PHI for a six year period.

Accountability
There are monetary penalties for violating privacy rules. Violations can include 1)discharge from employment 2) civil penalties of up to $25,000 per person and 3) Criminal penalties of up to $250,000 and/or 10 years in prison.

Restrictions
Describes when PHI can be used and when it cannot be used.

Public Responsibility
National health priorities such as public health, medical research, fraud and abuse investigations, clinical quality assessments and improvements may require the sharing of PHI without patient authorization.

Information Security
Sets up specific rules and standards for keeping patient information, written and electronic, confidential.

Protected Health Information (PHI)

The Privacy Rules protect all PHI from unnecessary disclosure:

- Relating to past, present or future medical condition or healthcare payment information of the individual.
- Created or received by a healthcare provider, health plan, employer life insurer, school or university.
- That could identify or be used in finding the identity of the individual.

Examples of PHI

- Name
- Birth date
- Social security number
- Driver's license number
- Fax machine number
- Zip code
- Photographs
- E-mail address
- License plate number
- Health insurance numbers
- Medical record number
- Financial account number

Is Only Written Information Covered by the Privacy Rules? NO!!!

Privacy Rules apply to:
 Electronic/computer information
 Paper records including nurses and doctor's notes
 Film, such as x-rays
 Verbal information including discussions in the cafeteria or over the telephone.

Authorization

 Privacy Rules permit sharing of PHI for purposes of **T**reatment, obtaining **P**ayment for services and business **O**perations (auditing, quality monitoring, etc.) **TPO**
 Permits sharing of PHI in cases of "national priorities" or Federal and/or State laws e.g., Anthrax or other epidemics, suspected child abuse.
 All other sharing of PHI must be authorized by the patient. A signed authorization form must be submitted before any information is disclosed to another person or company.
 If you are not sure whether you should give out any form of PHI, ask your supervisor, compliance representative, Privacy Officer or Compliance Officer.

Minimum Necessary Standard

The minimum necessary standard requires healthcare providers:
 To disclose the minimum amount of information requested.
 To allow workers access to the minimum amount of PHI necessary for them to do their jobs efficiently and effectively. This standard does not apply for treatment purposes.
 To access PHI and other information consistent with the person's role in the organization. A clinical nurse must have more access to clinical information than an accountant because of their role as a caregiver. However, the nurse should have automatic access to all clinical information on only the patients under her/his direct care.
Access to PHI or other patient information must be on a need-to-know basis.

Privacy Notice and Privacy Policy

 Privacy Rules require every healthcare provider to develop a statement on how the provider treats information. This is our Privacy Notice.

 Provider must make a reasonable effort to have our patients sign a form acknowledging they have received the Privacy Notice.

 Every provider must develop a Privacy Policy.

 Please take a few minutes and read the Privacy Notice and Privacy Policy included in your working notebook.

Privacy Officer

 Every provider must designate a Privacy Officer to oversee the adoption of written policies and procedures for compliance with HIPAA privacy regulations.

Disclosure of PHI

 Disclosing a patient's PHI is a daily occurrence.

 Most disclosures **DO NOT** require an authorization by the patient.

 Disclosures typically fall into three broad categories:

• Those made for **T**reatment, **P**ayment or Health Care **O**perations (**TPO**). **Do not require recording for an accounting.**

• Those made for other uses permitted by the Privacy Rules i.e., public health, national priorities, etc. **These must be recorded to allow for an accounting.**

• Those made by patient authorization. **Do not require recording for an accounting.**

Treatment, Payment or Healthcare Operations (TPO).

Do not require recording for an accounting.

 Treatment – provision, coordination or management of health care and related services by one or more health care providers.

 Payment – includes activities of a health care provider to obtain payment for services provided.

 Health Care **O**perations – includes quality assessment activities, competency assurance activities i.e., credentialing and accreditation, conducting medical reviews, audits, or legal services, insurance functions of risk rating or underwriting, business planning or development, management and general administrative activities.

 A covered entity may use and disclose **PHI**, **without**

authorization, for its own **TPO** activities.
 A covered entity may disclose **PHI**, **without authorization**, to another covered entity or health care provider for **TPO** activities if both entities have or had a relationship with the patient and the **PHI** pertains to the relationship.
 DOES NOT include most uses or disclosures of psychotherapy notes.

Other Uses Permitted by the Privacy Rules

These must be recorded to allow for an accounting.

` The Privacy Rules permit the use and disclosure of **PHI WITHOUT an Authorization** for 12 national priority purposes.

- Required by law - statute, regulation or court order
- Public health activities – public health authorities charged with controlling disease, injury or disability
- Victims of abuse, neglect or domestic violence
- Health oversight activities – audits, reviews and Investigations
- Judicial or administrative proceedings – requests through an order from a court or administrative tribunal
- Law enforcement – as required by law, to identify or locate a suspect, fugitive, material witness or missing person, a law enforcement official's request for information about a victim or suspected victim of a crime, to alert law enforcement of a person's death if the covered entity suspects criminal activity caused the death, if the covered entity believes the PHI in question is evidence of a crime that occurred on its premises, in a medical emergency when necessary to inform law enforcement about the commission, location, victim, or perpetrator of the crime
- Decedents – to funeral directors as needed and coroners or medical examiners to perform functions required by law
- Cadaveric organ, eye or tissue donation – to facilitate the donation and transplantation of organs, eyes and tissue
- Research purposes – with approval of the Institutional Review Board (IRB), with certification from the researcher that the disclosure is only for the preparation of the research protocol, is necessary for the project
- To avert serious threat to health or safety – to prevent or lessen a serious threat to a person or the public.
- Specialized government function – for national security activities, protective services to the President, protecting the health and safety of inmates or employees in a correctional institution.
- Workers' compensation – to comply with laws and regulations providing benefits for work-related injuries or illnesses.

 If you are not sure whether you should give out any form of PHI, ask your supervisor, compliance representative, Privacy Officer or Compliance Officer.

Accounting for Disclosures

Privacy Rules give individuals the right to request a listing of where their PHI was:

* Disclosed for a six-year period starting 4/14/03.

 ALL disclosures that are made under the other permitted disclosures must be recorded and include:

- Date of the disclosure
- Name of the entity or person who received the PHI and their address if known
- A brief description of the PHI disclosed
- A brief statement of the purpose for the disclosure or a copy of the written request for disclosure or other disclosure document

Disclosures Authorized by the Patient

Do not require recording for an accounting.

 A completed authorization form **MUST** be obtained:

- For any use that is not TPO
- For any use that does not fall within the 12 categories of other permitted uses
- Psychotherapy notes created by another party
- Treatment cannot be conditioned on receiving a signed authorization

 Examples:

- Disclosures to a life insurance company for coverage purposes
- Disclosures to an employer for the results of a pre-employment physical or lab test
- Disclosures to a supplier for their own marketing purposes

Minimum Necessary Standard

 The minimum necessary standard is applied to all uses and disclosures of PHI.

 Use or disclose the minimum amount of information requested.

 Minimum Necessary Standard **DOES NOT** apply to:

- Disclosure for treatment purposes
- Disclosure to the individual who is the subject of the information or his/her personal representative

• Disclosure to Health & Human Services (HHS) for complaint investigation, compliance review or enforcement
• Disclosures require by law • To allow workers access to the minimum amount of PHI necessary for them to do their jobs efficiently and effectively.

Things to Consider Before you Disclose PHI

 The Privacy Rules are not "black and white" on the use and disclosure of PHI.
Examples:
• Minors' rights – usually do not need an authorization to disclose PHI to a parent or legal guardian
• In emergency situations
• **An authorization is required** if the minor is emancipated (formal court document), required by state law for treatment in the areas of family planning, mental health, HIV, and sexually transmitted diseases.

 The Privacy Rules allow for the use your professional judgment in those instances that do not require authorization.

 Always take time to verify the identity of the person requesting the disclosure of PHI. Ask:
• If the patient is present, will he/she give verbal verification to disclose PHI to a person involved in their care
• The patient to verify over the telephone that you can disclose PHI to a person involved in their care

 Think before you disclose PHI.
• Is the disclosure for reasons of TPO?
• Is the disclosure permitted by the Privacy Rules?
• Does the disclosure require an authorization?
• Are you comfortable that the person requesting the disclosure of PHI is permitted to receive it under TPO, or other permitted uses?

Privacy Questions can be sent to:

 The Privacy Officer is Jason Williams and can be contacted at telephone number (850)415-6000 or (850)258-1580.

 The HIPAA e-mail address is: UltraJ_2000@yahoo.com

 The Compliance Officer is Jason Williams and can be contacted at telephone number (850)258-1580.

 The Compliance Hotline is 850-591-7014

What Does This All Mean to Me?

 Our patients have a right to expect we will keep their information confidential. This information includes anything that **could** identify or be used to find out the identity of the patient or their medical condition.

 As employees, volunteers and physicians, we come in contact with many forms of patient information, i.e. surgical lists, laboratory draw lists, patient census listings, etc. We need to understand what are acceptable uses of this information.

 Follow the "need to know" rule. Ask yourself "do I need to see patient information to perform my job". If the answer is "Yes", you have nothing to worry about. If the answer is "no", **STOP**.

 The cafeteria or elevator is not the place to discuss the medical condition or other aspects of a patient's care.

 Information you have access to must not be the subject of conversation with family, friends or neighbors.

 Most disclosures of PHI do not need an authorization by the patient. PHI can be disclosed **without** an authorization for reasons of TPO and any of the 12 permitted uses under the Privacy Rules. Any other disclosure requires an authorization by the patient.

 The minimum necessary standard needs to be applied to all disclosures except for treatment purposes, disclosures to the patient or as required by law.

 All disclosures except for reasons of TPO or those authorized by the patient **must** be recorded to allow for a requested accounting of disclosures.

 Confidentiality of all patient information is a serious matter.

 Violations of confidentiality and privacy policies can result in disciplinary action up to and including discharge.

 If you know of any violation of our existing confidentiality policies or the Privacy Policy, it is your obligation to bring the violation to the attention of your supervisor, compliance representative, Privacy Officer or Compliance Officer.

Compliance Is Not An Option!

I have read and received a copy of the HIPAA and Privacy regulations.

_____ _____

Signature **Date**