HIPAA RULES

ARE YOU COMPLIANT ?

September 30, 2021

Why was HIPAA Created?

HIPAA was created **to "improve the portability and accountability of health insurance coverage" for employees between jobs**. ... The procedures for simplifying the administration of health insurance became a vehicle to encourage the healthcare industry to computerize patients´ medical records.

The Four Primary Objectives of HIPAA

1 - Assure health insurance portability by elimination of job-lock due to pre-existing medical conditions.

Job lock happened when people with preexisting health conditions **were afraid to leave one job with insurance for another job with** insurance because the new insurance would not cover their condition, or would impose long waiting periods.

2 - Reduce healthcare fraud and abuse.

3 - Enforce standards for health information.

4 - Guarantee security and privacy of health information.

Who must follow HIPAA?

The following entities must follow HIPAA regulations. The law refers to these as "covered entities":

- Health plans
- Health care providers, including doctors, medical staff, clinics, hospitals, nursing homes, and pharmacies
- Health care clearinghouses

HIPAA also applies to covered entities' business associates.

Examples of a Potential Business Associates

Data processing firms or software companies that may be exposed to or use PHI:

- Medical equipment service companies handling equipment that holds PHI
- Shredding and/or documentation storage companies
- Consultants hired to conduct audits, perform coding reviews
- Lawyers
- Answering services
- Medical transcription services
- e-prescribing services

What is a Business Associate?

A Business Associate is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to a covered entity.

You must have all your Business Associates sign a Business Associate Agreement.

The HIPAA Security Rule

The HIPAA Security Rule **establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity**.

The HIPAA Security Rule requires three kinds of safeguards: **administrative, physical, and technical**.

Examples of these safeguards

Administrative: Employee Training and having written policy's in place.

Physical: Locked doors and signs labeling restricted areas.

Technical: Encryption. Antivirus and Anti-Malware Software. Firewalls.

The HIPAA Privacy Rule

The HIPAA Privacy Rule **establishes national standards to protect individuals' medical records and other personal health information** and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically.

Privacy Rule
Permitted Uses & Disclosures

Only 3 Types of Disclosures Are Permitted Under the HIPAA Laws

1 - Required – Government (HHS, OCR, OIG)

Government does not include law enforcement

2 - Permitted:

Uses and disclosures between covered entities.

Uses and disclosures to a Business Associate.

Uses and disclosures pursuant to a valid HIPAA Authorization.

3 - Authorized – Patient Not Subject to Minimum Necessary

The Privacy Rule permits covered entities to disclose protected health information, without authorization, to public health authorities who are legally authorized to receive such reports for the purpose of preventing or controlling disease, injury, or disability.

HIPAA Risk Assessment Is this Required?

Yes, The HIPAA Security Rule requires Covered Entities and their Business Associate to conduct an annual HIPAA risk Assessment and implement security measures in order to help safeguard PHI.

What is contained in a Risk Assessment?

Your Risk Assessment is broken down into 3 key areas and your responses to the questions in each area will help you create your Policies and Procedures.

1 – Administrative Safeguard - Here you list your administrative requirements that include answering questions about your;

- **Sanction Policy for employees that violate your policies;**
- **Policies and Procedures review schedule and,**
- Plan for dealing with Breaches

2 – Technical Safeguards - How does your practice or company protect ePHI? Do you have:

- A data backup plan
- A disaster recovery plan
- An emergency mode of operation plan

3 – Physical Safeguards - This area deals with physical files, and how you protect your offices.

- Who has access to your location?
- How do you protect patient or client files?
- How do you control who has access to physical files?

The Risk Assessment is a living document, and the first year you have this in place, you may find certain parts work, and others don't. This means you need to update the document to reflect any changes you make along the way.

Patients Rights Mandated by HIPAA

Patients have the right to:

- Receive the Notice of Privacy Practice (Have all patients read and resign this form every 3 years)
- Access their medical record
- Request amendments to their medical record
- An accounting of disclosures of their medical records
- Request restriction on release of Protected Health Information
- **File a complaint (Please take your patients complaints very serious! The last thing you want is a call to Health and Human Services)**

What is Protected Health Information

PHI stands for Protected Health Information and is **any information in a medical record that can be used to identify an individual**, that was created, used, or disclosed in the course of providing a health care service, such as a diagnosis or treatment.

PHI includes patient identifiers such as:

- Names
- Address and Phone/Fax Number
- Date of Birth
- Medical Record Number
- Social Security Number
- Employer
- Diagnosis, Medical History, Medications
- Surgical and other procedures
- Insurance/Health plans, billing records
- Email address and Photographs

Release of Patient Protected Health Information (PHI)

When is an Authorization Form required from the patient?

When the release of PHI is for non Treatment, non Payment and non Healthcare operations.

When a patient request a copy of their medical record including images, test results etc.

When the patient request ePHI (electronic PHI) be sent to a third party.

Prior to releasing PHI information to the media or for public display;

or when the release of PHI is to an attorney.

Permitted Uses & Disclosures

A covered entity is permitted, but not required, to use and disclose protected health information, without an individual's authorization, for the following purposes or situations:

- **To the Individual (unless required for access or accounting of disclosures);**
- **Treatment, Payment, and Health Care Operations (Continuity of Care);**
- **Serious Threat to Health or Safety**
- **Essential Government Functions**
- **Workers Compensation**

Communicating with Family & Friends

Disclosure to patients, family, friends and caregivers.

The HIPAA Privacy Rule **permits covered entities to share information** that is directly relevant to the involvement of a spouse, family members, friends, or other persons identified by a patient, in the patient's care or payment for health care.

The provider or plan can share your information with family or friends if:

- However, the provider or plan can share your information with family or friends if:
- They are involved in your health care or payment for your health care,
- The patient tells the provider or plan that it can do so,
- You do not object to sharing of the information, or
- If, using its professional judgment, a provider or plan believes that you do not object.

Request for Confidential Communications

Covered health care providers must permit individuals to request an alternative means or location for receiving communications of protected health information by means other than those that the covered entity typically employs.

For example, an individual may request that the provider communicate with the individual through a designated address or phone number.

Different Address

Unmarked Envelope

Request For Restrictions

An individual has the right to request a restriction on the use or disclosure of his or her PHI (a) for treatment, payment, or health care operations, and (b) disclosures to family and friends involved in the individuals care.

When an individual request a restriction, the person requesting the restriction should complete the "Request to Restrict Uses and Disclosures of Protected Health Information" form. Place the completed form in the patient's medical record.

Giving Patients Control over their information

- Only share patient information with other faculty and staff who need the information to do their job.

- Avoid accessing a patient's record unless you need to do so for your job or you have written permission from the patient. *You are not allowed to access the record of your co-worker, spouse, or family member unless there is a signed authorization form in the patients record.*

HIPAA & Patient Self-Pay

Thanks to HIPAA/HITECH regulations you now have the ability to have a patient opt out of filing their health insurance. If a patient elects to opt out of their insurance you need to have them sign an election to self-pay form.

The Social Security Act states that participating providers must bill Medicare for covered services. The **only time a participating-provider can accept "self-payments" is for a non-covered service**.

Why Do We Need to Protect PHI?

- It's the law.
- To protect the reputation of your practice.
- To avoid potential withholding of federal Medicaid and Medicare funds.
- To build trust between providers and patients.

Who or What Protects PHI?

The Federal Government protects PHI through HIPAA regulations.

HIPAA Violations are Expensive

The penalties for non compliance are based on the level of negligence and can range from $100 to $50,000 per violation (or per record) with a maximum penalty of $1.5 million per year for violations of an identical provision.

A Florida-based health system accesses unauthorized PHI, revealing numerous HIPAA violations.

- In Florida, a health system received a $2.15 million civil penalty from the Office for Civil Rights after violating several HIPAA rules, including impermissible disclosure of PHI, risk analysis failures, infrequent reviews of information system activity, and unauthorized and intentional access to patient's medical information for selling purposes. They also neglected to notify individuals of a potential breach when a box of files went missing and they failed to report this for 160 within 60 days, as required by law.
- **Lesson to learn:** Every hospital, medical center, and health system needs to prioritize HIPAA compliance and make reasonable efforts to prevent, detect, and correct HIPAA violations or they can expect to pay a significant financial price.

Criminal Penalty for a HIPAA Violation

The maximum criminal penalty for a HIPAA violation by an individual is $250,000….. Knowingly violating HIPAA Rules with malicious intent or for personal gain can result in a prison term of up to 10 years in jail. There is also a mandatory two-year jail term for aggravated identity theft.

10 Most Common HIPAA Violations

1-Unsecured Records Containing PHI
2-Unencrypted Data
3-Data Breaches
4-Improper Disposal of Patient Records
5-Insufficient or Lack of Employee Training
6-Unauthorized Release of Patient Information
7-Failure to Perform a Risk Assessment
8-Oversight in Entering HIPAA-Compliant Business Associate
9-Missing the 60 Day Deadline for Issuing Breach Notification
10-Unauthorized Access to Patient Records

- Releasing information to an undesignated party is a HIPPA violation scenario. Only the exact person listed on the authorization form may receive patient information. If a patient authorizes his or her mother to receive medical information, she is the only person the information can be shared with.

- Releasing unauthorized health information is also a violation. This refers to releasing the wrong document that has not been approved for release. A patient has the right to release only parts of their medical record.

How are the HIPAA Regulations Enforced?

- The public. The public is educated about their privacy rights and will not tolerate violations. They will take action!
- Office For Civil Rights (OCR). The agency that enforces the privacy regulations providing guidance and monitoring compliance.
- Department of Justice (DOJ). Agency involved in criminal privacy violations. Provides fines, penalties and imprisonment to offenders.

Privacy Officer

HIPAA says that **every practice** or healthcare organization **must** designate a **privacy officer**.

No office - no matter it's size – is not exempt from this HIPAA requirement. In larger **healthcare** organizations, It's not uncommon for the role of the **HIPAA Privacy Officer** to be someone's entire job.

Some of the Duties of a Privacy Officer

- Keeping up-to-date on federal and state privacy laws
- Maintaining a record of each patient's acknowledgment of receiving the Notice of Privacy Practices (NPP)
- Meeting request from patients for access to their health records
- Meeting request from patients for corrections or change to their health records
- Providing information to patients or staff who have questions about HIPAA and their privacy protections
- Dealing with complaints from patients and staff about possible HIPAA violations
- Keeping track of your Business Associate Agreements

Members of the workforce who handle PHI require training!

- Required upon hire and recommended annually
- As material changes are implemented training to appropriate workforce members affected by that change
- Documentation of the training who attended, the topic covered and date the training was held

HIPAA Breach Risk Assessment

at a minimum the following four factors must be reviewed and documented:

- The nature and extent of the PHI involved and the likelihood of re-identification
- The unauthorized person to whom the discloser was made;
- Where the PHI was actually acquired or viewed; and
- The extent to which the risk to the PHI has been mitigated.

HIPAA Breach

any impermissible acquisition access, use or disclosure of unsecured PHI is presumed to be a breach…

HIPAA Breach Risk Assessment

at a minimum the following four factors must be revised and documented:

- **The nature and extent of the PHI involved and the likelihood of re-identification;**
- **The unauthorized person to whom the disclosure was made;**
- **Where the PHI was actually acquired or viewed; and**
- **The extent to which the risk to the PHI has been mitigated.**

The Breach Notification Rule

The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, **requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information**.

Once a covered entity knows or by reasonable diligence should have known (referred to as the "date of discovery") that a breach of PHI has occurred, the entity has an obligation to notify the relevant parties (individuals, HHS and/or the media) "without unreasonable delay" or **up to 60 calendar days following the date** ...

Notify the HHS/OCR and the Media

- You must notify the HHS/OCR of the breach. So, if the breach has affected less than 500 individuals, you should maintain an annual breach log and submit the same within 60 days of the year ending. On the other hand, if the affected individuals number more than 500, you must notify the HHS/OCR at the same time as when you notify the affected individuals.
- **Notify the media**
- You only need to notify the media if the breach involves more than 500 individuals in the same state or jurisdiction. In case you need to notify the media, you need to do so by sending a press release with the same information you sent to the affected individuals in that same area. The media must be notified within 60 days of discovering the breach.

Access Initiative

A covered entity may not impose unreasonable measures on an individual requesting access that serve as barriers to or unreasonable delay the individual from obtaining access. For example, a doctor may not require an individual:

- **Who wants a copy of her medical record mailed to her home address to physically come to the doctor's office to request access and provide proof of identity in person.**
- **To use a web portal for requesting access, as not all individuals will have ready access to the portal.**
- **To mail an access request, at this would unreasonably delay the covered entity's receipt of the request and thus, the individuals access.**

Communication with Family & Friends

Disclosures to patients, family, friends and caregivers.

HIPAA allows health care professionals to disclose some health information without a patient's permission under circumstances, including:

Sharing health information with family and close friends who are involved in care of the patient if the provider determines that doing so is in the best interest of an incapacitated or unconscious patient and the information shared is directly related to the family or friend's involvement in the patient's health care or payment of care.

Just a quick summary

It's your job to protect all information that can be used to connect the patient to their health information.

- The minimum necessary rule states: You should use or disclose the least amount of PHI to get the job done.
- Use and discloser of protected health information is required when it is requested or authorized by the patient or when required by Health and Human Services.
- A signed authorization from the patient is required for use and discloser of protected health information.
- In regards to The HIPAA Security Rule: The three safeguards we use that cover all procedures and systems, to protect electronic Protected Health Information are: Administrative, Physical and Technical
- A breach is any unauthorized use or discloser of PHI.
- **Do not use your work computer for personal use. Do not download anything unauthorized, Don't use unencrypted flash drives, no personal email , do not connect your cell phone to your work PC. Please keep your work P.Cs secure. The vulnerability for Malware, Ransomware and viruses are real, also make sure you use passwords that are not easily figured out and change them regularly. Remember if your patient information is compromised electronically . It's a Breach!**

Thank you !

Q & A

MSD offers in-person HIPAA/OSHA & BLS training

Contact Dwayne Downs

302-494-4220

dwayne.downs@medsocdel.org