HIPAA IN CLINICAL TRAILS

DEFINITION

- HIPAA is defined as the Health Insurance Portability and Accountability Act (HIPAA) is a federal law that provides baseline privacy and security standards for medical information. The U.S. Department of Health and Human Services (HHS) is the federal agency in charge of creating rules that implement HIPAA and also enforcing HIPAA.

BRIEF HISTORY

- 1996 – Congress passed the Health Insurance Portability and Accountability Act (HIPAA).

- 2003 – The U.S. Department of Health and Human Services (HHS) issued and adopted the HIPAA Privacy Rule, HIPAA Security Rule, and the HIPAA Enforcement Rule.

The **Privacy Rule** gives individuals rights with respect to their protected health information (PHI). It also explains how covered entities (those who must comply with HIPAA) can use and disclose PHI.

- The **Security Rule** sets standards for safeguarding electronic PHI. the Security Rule laid down three security safeguards – administrative, physical and technical – that must be adhered to in full in order to comply with HIPAA. The safeguards had the following goals:

Administrative – to create policies and procedures designed to clearly show how the entity will comply with the act.

Physical – to control physical access to areas of data storage to protect against inappropriate access.

Technical – to protect communications containing PHI when transmitted electronically over open networks.

The **Enforcement Rule** addresses compliance, investigations, and potential penalties for violations of the HIPAA Privacy Rule and Security Rule. The Office for Civil Rights (OCR) within HHS is reponsible for enforcing the HIPAA regulations.

- **2009 – The Health Information Technology for Economic and Clinical Health (HITECH) Act was signed into law.**

The HITECH Act created financial incentives for healthcare providers and insurers to continue shifting to electronic medical records, and also addressed privacy and security concerns related to the electronic transmission of health information, including unauthorized access and data breaches.

- **2013 – HHS' Office for Civil Rights issued the HIPAA Omnibus Rule.**

HHS' Omnibus Rule made several important changes to the HIPAA Privacy, Security, and Enforcement Rules. It implemented many provisions of the HITECH Act. It modified and finalized the Breach Notification Rule. It also implemented changes to the HIPAA Privacy Rule required by the Genetic Information Nondiscrimination Act of 2008 (GINA).

WHO MUST COMPLY WITH HIPAA?

- HIPAA only applies to covered entities and their business associates. Some times a subcontractor can also be considered.

a. Covered entities: The Privacy Rule defines a Covered HIPAA Entity as any health plan or any healthcare clearinghouse, or any healthcare provider who transmits Protected Health Information (or PHI as per the standards developed by the Department of Health & Human Services) in electronic form.

Health care providers get paid to provide health care Doctors, dentists, hospitals, nursing homes, pharmacies, urgent care clinics, and other entities that provide health care in exchange for payment are examples of providers.

Health plans pay the cost of medical care. The following are examples of health plans covered under HIPAA: health insurance companies, health maintenance organizations (HMOs), group health plans sponsored by an employer, government-funded health plans such as Medicare and Medicaid, and most other companies or arrangements that pay for health care.

Health care clearinghouses process information so that it can be transmitted in a standard format between covered entities. For example, a clearinghouse may take information from a doctor and put it into a standard coded format that can be used for insurance purposes.

b. Business associates : A "business associate" creates, receives, maintains, or transmits protected health information (PHI) on behalf of a covered entity .

c. Subcontractors: A subcontractor that creates, maintains, or transmits protected health information (PHI) on behalf of a business associate has the same legal responsibilities as a business associate under HIPAA. In other words, privacy- and security-related legal responsibilities flow "downstream" to subcontractors performing work for a business associate.

For example, a hospital's business associate may hire an outside company to shred documents containing PHI or to provide a cloud service to store the data.

PROTECTED HEALTH INFORMATION(PHI)

- Under HIPAA PHI is considered to be any identifiable health information that is used, maintained, stored, or transmitted by a HIPAA-covered entity – A healthcare provider, health plan or health insurer, or a healthcare clearinghouse – or a business associate of a HIPAA-covered entity, in relation to the provision of healthcare or payment for healthcare services.
- PHI is health information in any form, including physical records, electronic records, or spoken information.
- Therefore, PHI includes health records, health histories, lab test results, and medical bills. Essentially, all health information is considered PHI when it includes individual identifiers

- **The HIPAA Privacy Rule** regulates the use and disclosure of protected health information (PHI) by "covered entities.“

Use: How information is used within a healthcare facility.

Disclosure: How information is shared outside a health care facility.

- Covered entities may disclose PHI to law enforcement if requested to do so by court orders, court-ordered warrants, subpoenas, and administrative requests.
- A covered entity may reveal PHI to facilitate treatment, payment, or health care operations without a patient's written authorization.

- Any other disclosures of PHI require the covered entity to obtain prior written authorization.
- When a covered entity discloses PHI, it must make a reasonable effort to share only the minimum necessary information.
- The Privacy Rule gives individuals the right to demand that a covered entity correct any inaccurate PHI and make reasonable steps to ensure the confidentiality of communications with individuals.
- The Privacy Rule requires covered entities to notify individuals of PHI use, keep track of disclosures, and document privacy policies and procedures.

MINIMUM NECESSARY STANDARD(MNS)

This rule stipulates that the disclosure of PHI must be limited to the minimum necessary for the stated purpose. Exceptions to the rule exist in a healthcare environment

- where it may be necessary for a healthcare provider to access a patient´s complete medical history – but non-routine disclosure requests must be reviewed on a case-by-case basis.
- even when the patient has given their authorization for their medical records to be made available for research, marketing or fundraising purposes.
- In interest of public health like to control or prevent disease.
- Signed patient authorization is necessary for the use/disclosure of psychotherapy notes unless required by healthcare provider or required by law.

The Health Insurance Portability and Accountability Act of 1996 consists of 5 Titles.

- Title I: Protects health insurance coverage for workers and their families that change or lose their jobs. It limits new health plans the ability to deny coverage due to a pre-existing condition.
- Title II: Prevents Health Care Fraud and Abuse; Medical Liability Reform; Administrative Simplification that requires the establishment of national standards for electronic health care transactions and national identifiers for providers, employers, and health insurance plans.
- Title III: Guidelines for pre-tax medical spending accounts. It provides changes to health insurance law and deductions for medical insurance.
- Title IV: Guidelines for group health plans. It provides modifications for health coverage.
- Title V: Governs company-owned life insurance policies. Makes provisions for treating people without United States Citizenship and repealed financial institution rule to interest allocation rules.

HIPPA COMPLIANCE IN CLINICAL TRAILS

- The federal Medical Privacy Rule, authorized by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), limits how covered physicians may use and disclose protected health information (PHI) for any purpose.
- Throughout the clinical study process, researchers may need to create, edit, and view PHI. HIPAA stipulates that participant PHI must be used in a "specific and meaningful manner."
- All study participants must submit authorizations in order for the researchers to have access to their pertinent information. This authorization only applies to the current study, and not to any future studies.

1. Pre-Research Review of Medical Records

- A prospective sponsor might request summary information about a physician's patients to establish whether the physician's practice is a viable site for a clinical trial.
- The Privacy Rule permits the physician to review her medical records for this "pre-research" purpose, provided that no PHI is disclosed to the sponsor.
- If a third party, such as a contract research organization (CRO) or another researcher will review medical or billing records for this purpose, the review must occur at the practice and the physician must obtain the following representations: The use or disclosure is sought solely to review PHI as necessary to prepare a research protocol or for similar purposes preparatory to research:
- No PHI will be removed from the covered entity during the review; and
- The PHI that the researcher [or CRO] seeks to review is necessary for the purpose(s) of the review.

- To document HIPAA compliance, the physician should ask the third party to provide these representations in writing.
- Alternatively, the Privacy Rule allows the physician to share "de-identified" data without restriction. The Privacy Rule's standard for de-identification is quite strict, typically requiring removal of eighteen specific identifiers that range from names and social security numbers to dates of treatment and full zip codes.
- The de-identification of protected health information enables HIPAA covered entities to share health data for large-scale medical research studies, policy assessments, comparative effectiveness studies, and other studies and assessments without violating the privacy of patients or requiring authorizations to be obtained from each patient prior to data being disclosed.

2. RECRUITMENT

- The Privacy Rule permits a physician to recruit her own patients, by, for example, sending a letter to patients potentially eligible to enroll in a clinical trial, or by discussing enrollment during an office visit. (The institutional review board overseeing the study must approve the recruitment plan.)
- If a CRO wishes to use a physician's records to recruit patients, the study's principal investigator should seek a partial waiver of HIPAA authorization from the institutional review board.

Uses and disclosures for which an authorization or opportunity to agree or object is not required;

(a) Uses And Disclosures Required By Law.

(B) Uses And Disclosures For Public Health Activities .

(C) Disclosures About Victims Of Abuse, Neglect Or Domestic Violence

(D) Uses And Disclosures For Health Oversight Activities -

(E) Disclosures For Judicial And Administrative Proceeding

(F) Disclosures For Law Enforcement Purposes.

(G) Uses And Disclosures About Decedents

- participants must first review certain documents to ensure a comprehensive understanding of the study. If you decide to participate in a clinical trial, you may be asked to sign two documents: an authorization form, and an informed consent document.
- The informed consent document will detail the study methodology, any potential risks, timeline, participant confidentiality and healthcare coverage during the course of the study. This document may or may not be combined with an authorization form.

A few elements that may be present in the authorization may include:

- Your health information will be disclosed when it is required by law
- Your health information will be shared when required by law, to prevent or control injury or the spread of disease
- No publication or public presentation about the study will reveal your identity
- To maintain the integrity of the study, you may not have access to your PHI until the study is complete.

You do not have to sign this authorization, but if you decline, you may not be eligible for study participation. Revoking this permission means you will no longer be eligible for participation within the clinical study.

3. Enrollment and Conduct of Study

- A physician generally must obtain written HIPAA research authorization to enroll a patient in a clinical trial.
- Though a research sponsor may provide a template consent form, typically the research site, which is the covered entity, must supply the HIPAA authorization.
- The study's authorization and consent forms are usually combined, which is permitted, provided that the combined form contains all of the elements required by both the Privacy Rule and federal research regulations.
- A HIPAA research authorization must contain all the elements of a valid general HIPAA authorization.

To be valid, a HIPAA authorization must satisfy the following :

1.No Compound Authorizations. The authorization may not be combined with any other document such as a consent for treatment.[3] An authorization to use or disclose psychotherapy notes may not be combined with an authorization to disclose other forms of PHI.

2.Core Elements: These include a description of the PHI to be used or disclosed that identifies the PHI in a specific and meaningful fashion.

- The name or specific identification of the person(s) or class of person(s) authorized to make the use or disclosure.
- The date and signature of the patient or the patient's personal representative.
- A description of each purpose for the requested use or disclosure.

3.Required Statements. The authorization must also contain certain required statements regarding **patient rights.**

- The patient or personal representative has the right to revoke the authorization at anytime by submitting a written revocation except to the extent the provider has taken action in reliance on the authorization.
- The provider generally may not condition its healthcare on the provision of the authorization except (i) for research-related treatment, or (ii) if the purpose of the healthcare is to create information for disclosure (e.g., an employment physical or independent medical exam), in which case the provider may refuse to provide the healthcare if the patient refuses to execute an authorization.
- The information disclosed per the authorization may be subject to re-disclosure by the recipient and no longer protected by HIPAA.

4. Marketing or Sale of PHI. If the authorization is to permit the use or disclosure of PHI for purposes of marketing (as defined by HIPAA) or the sale of PHI, and the provider will receive remuneration for the PHI, the authorization must notify the patient that the provider will receive the remuneration.

5.Completed in Full. The authorization and its required elements must be completely filled out, i.e., there should be no blanks concerning the required terms.

6.Written in Plain Language. The authorization must be written in plain language. For patients with limited English proficiency, the provider may need to translate the authorization for the patient.

7.Give the Patient a Copy. If the provider is requesting the authorization from the patient, the provider must give the patient or personal representative a signed copy of theauthorization. The provider is not required to give a copy if the patient initiated the authorization.

8. **Retain the Authorization.** The provider must retain a copy of the authorization for six years.

- If an authorization is required, HIPAA prevents providers and business associates from using or disclosing more PHI than is allowed or in a manner that is different than as stated in the authorization, so providers should ensure that the authorization is broad enough to cover the requested use or disclosure, including any disclosure of oral information in addition to records.
- Every HIPAA authorization must also tell the patient how to revoke authorization. If a patient does revoke authorization, the physician conducting the trial may continue to use and disclose (eg, provide to the research sponsor) PHI obtained before the revocation. After revocation the physician may use and disclose the patient's new PHI only as necessary to maintain the integrity of the research (eg, to report an adverse event or the death of a study subject).

4. Publication or Presentation of Results

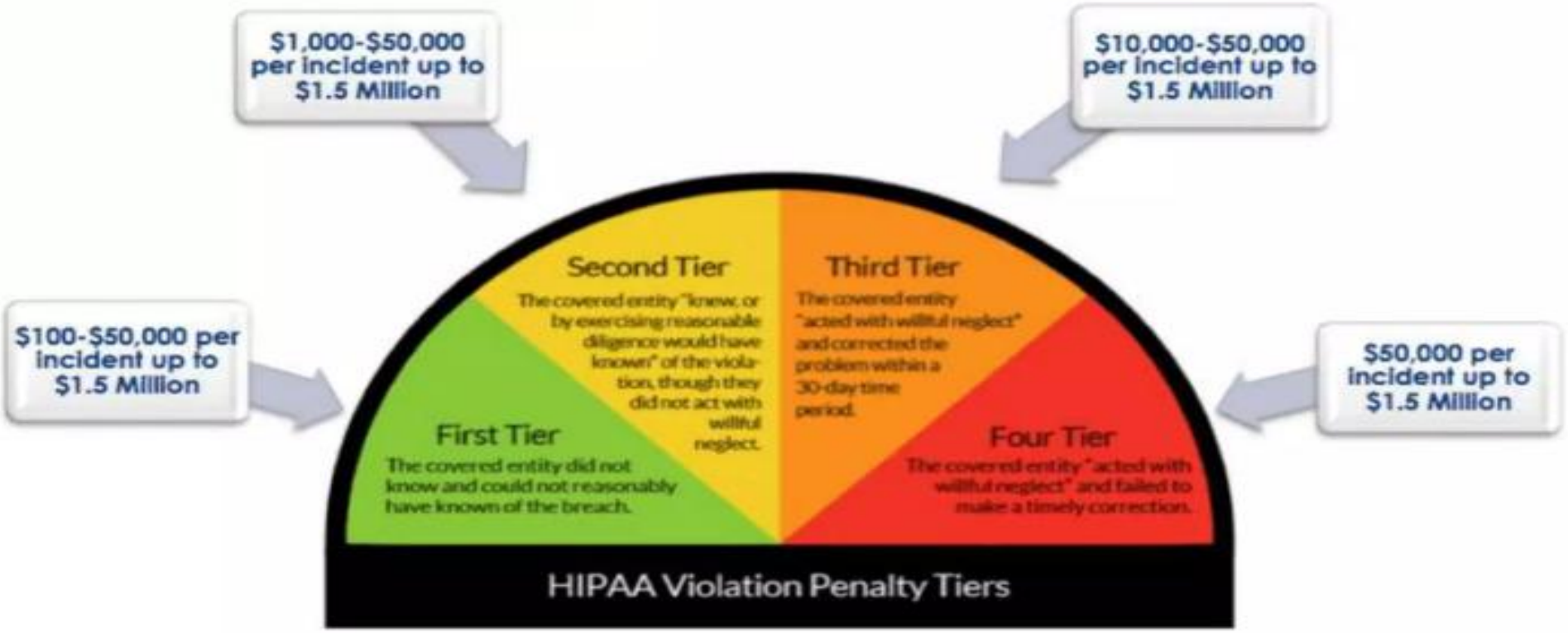
- HIPAA continues to apply when the results of clinical trials (or case studies) are published or presented to an audience. Except when conducting internal medical education activities, physicians must obtain written HIPAA authorization before publishing papers or making presentations containing PHI. An institutional review board may not waive authorization for the publication or presentation of research.
- Physicians whose publications or presentations will contain patient-level data should determine whether the eighteen HIPAA identifiers have been removed, and also whether the remaining information could be combined with other publicly-available information to reveal the identity of a participant. Materials involving photographs, rare diseases, or highly publicized cases should be reviewed with particular care.

What Happens if You Break HIPAA Rules?

If you break HIPAA Rules there are four potential outcomes:

- The violation could be dealt with internally by an employer.
- You could be terminated.
- You could face sanctions from professional boards.
- You could face criminal charges which include fines and imprisonment.

Penalties



CompliancyGroup

855.85HIPAA
www.compliancygroup.com