HIPAA Compliance

Clean CLAIM MD

WORKING HARD SO YOU GET PAID

www.cleanclaimmd.com

Disclaimer

HIPAA DEFINITIONS

Covered Entity
A health plan, clearinghouse, or provider who transmits any health information in electronic form in connection with a transaction covered under the HIPAA Administrative Simplification standards. Some examples of a covered entity are hospitals, insurance companies, or physician practices.

Business Associate
An entity that "creates, receives, maintains, or transmits protected health information" in a contractor role with a covered entity. Subcontractors are also business associates. Examples of business associates are information technology vendors or e-prescribing gateways.

Workforce
Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate.

Protected Health Information (PHI)
Individually identifiable health information (medical records, demographics, or payment data) that is transmitted by electronic media (data in motion, e.g. email), maintained in electronic media (data at rest, e.g. a database or laptop hard disk), or Transmitted or maintained in any other form or medium (e.g. oral or hard copy).

Breach
The acquisition, access, use, or disclosure of protected health information in a manner which compromises the security or privacy of the protected health information. With a few exceptions, such a disclosure is presumed to be a breach unless the covered entity or business associate is able to demonstrate that there is a low probability that the protected health information has been compromised based on a risk assessment.

What Is HIPAA?

- Health Insurance Portability and Accountability Act.
- Federal law designed to protect the privacy and security of patient information.
- Includes the following:
  - Privacy Rule
    - Prohibits the use/disclosure of patient information without patient authorization except in certain limited instances; sets forth certain patient rights.
  - Security Rule
    - Identifies a set of security safeguards (physical, technical, and administrative) that must be implemented to safeguard electronic patient information.
  - Breach Notification Rule
    - Addresses steps that must be taken when the privacy of patient information is breached.

To Whom Does HIPAA Apply?

- Covered Entities
  - Certain Health Care Providers
  - Health Plans
  - Health Care Clearinghouses
- Business Associates of Covered Entities

Health Care Providers

- Broad definition that includes: Doctors, Clinics, Psychologists, Dentists, Chiropractors, Nursing Homes, Assisted Living Facilities, Pharmacies.

- BUT only if they transmit information in electronic form in connection with an electronic standard transaction which HHS has adopted a standard.
  - Basically means that the health care provider has to communicate electronically with health plans/payors (e.g., request for payment, eligibility check, prior authorization, etc.).

Health Plans

- Health insurance companies.
- HMOs.
- Company health plans.
- Government programs that pay for health care (Medicare/ Medicaid, others).

Health Care Clearinghouses

- Entities that process nonstandard health information into a standard format.
- Classic example – billing company that receives Medicare claims and converts them to a format that Medicare's electronic system will understand.

Business Associates

- A person or organization that is NOT CE Workforce.
- Performs functions on behalf of CE or provides services to CE.
- Where access to PHI is involved.
- Examples: legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, financial services.

Subcontractors

- The definition of “Business Associate” includes a “subcontractor that creates, receives, maintains or transmits PHI on behalf of the business associate.”
- A subcontractor is a person to whom a BA has delegated a function, activity or service that the BA has agreed to perform for the CE.

What Does HIPAA Cover?

- Protected Health Information (PHI).
- Relates to the past, present or future:
  - physical or mental health condition of an individual;
  - provision of health care to an individual; or
  - payment for the provision of health care to an individual
- Includes both oral or recorded information.
- Electronic or paper - any form.

NOT Covered by HIPAA

- Information that has been "de-identified."
  - De-identification requires a specific process under HIPAA (not just removing the patient's name).
- Employment records.
- Education records (Family Education Rights and Privacy Act).
- Information regarding individuals who are deceased for more than 50 years (but state laws may still protect that information).

The General Rule Under HIPAA

- Do not use or disclose PHI without written patient authorization.
  - Use = within CE.
  - Disclosure = outside CE, even to business associates.

- HIPAA carves out exceptions where PHI may be used or disclosed, i.e., where the general prohibition does not apply.

Major Exceptions To Privacy Prohibition

- To the patient (or legal representative).

- TPO
  - Treatment – provision, coordination, management of care/related services including consults and referrals.
  - Payment for health care – reimbursement for health care, coverage, all related activities.
  - Health care operations – slide coming up.

Exception – Health Care Operations

- Quality assessment and improvement.
- Competency assurance, peer review, credentialing.
- Audits, legal or medical reviews, compliance.
- Insurance functions.
- Business planning, development, management administration.
- General administrative activities including de-identification and creating limited data sets.

Exceptions – Opportunity to Agree or Object

- Facility directories (may disclose condition and location in facility to those who ask by name, and religious affiliation to clergy).

- Family/ friends – disclosure okay if relevant to that person's involvement in care or payment for care.
  - Example: your spouse can pick up your prescriptions from the pharmacy.

Exception – Incidental Disclosures

- At times it is unavoidable that some people will hear PHI (but must try to limit).

- Examples (these are not violations under HIPAA):
  - Nurse A standing near Nurse B overhears B's conversation with a patient on the phone involving PHI.
  - Staff Member A and Staff Member B print at the same time. Staff Member A's document contains PHI. Staff Member B inadvertently views A's document while trying to obtain his own document.

Other Major Exceptions To Privacy General Prohibition

- Where required by law (e.g. child abuse reporting).
- Certain communications about decedents.
- Public Health Agencies (like CDC).
- Health Oversight Agencies (like DHHS).
- Disaster/ Emergency.
- Clinical Research (with lots of caveats).

Other Major Exceptions To Privacy Prohibition

- Judicial and Administrative Proceedings.
- Certain Disclosures to Law Enforcement.
- Serious Threat to Health or Safety.
- Essential Government Functions.
- Workers' Compensation.
- Limited Data Set.

Limited Data Set

- PHI from which specified direct identifiers have been removed.
- May be used and disclosed for research, health care operations, and public health purposes.
- PROVIDED THAT THERE IS A DATA USE AGREEMENT WITH SPECIFIED SAFEGUARDS.

Minimum Necessary Rule

- HIPAA requires CEs and BAs to limit the use or disclosure of PHI to the minimum necessary to accomplish the purpose of the use or disclosure.
  - For example, if you don't need to disclose an entire file or patient record – only disclose the limited portions that you need to disclose.
- Certain exceptions (e.g., treatment, pursuant to authorization, required by law, etc.)
- HHS expected to issue additional guidance.

Marketing, Sale of PHI, Fundraising

- Marketing – very complicated.
- Sale of PHI – lots of exceptions.
- Fundraising
  - CE may use or disclose to a BA or an institutionally related foundation certain PHI for fundraising without a patient authorization!
  - Each fundraising communication must provide "clear and conspicuous" opportunity to opt-out that does not cause an undue burden or more than a nominal cost (good: toll free number; bad: writing a letter).
  - NPP must state CE may contact individuals to raise funds for the CE and that the individual has a right to opt out.

Patient Rights Under HIPAA

- Right to Access.
- Right to Request Amendment of PHI.
- Right to Request Restrictions on Uses and Disclosures of PHI.
- Right to Request Confidential Communications.
- Right to an Accounting of Disclosures.
- Right to Complain About Disclosures.
- Notice of Privacy Practices.

Request for Access

- Individual's have right to inspect and obtain a copy of the individual's PHI the CE/BA maintains in a Designated Record Set.
- If an individual requests an electronic copy of PHI that is maintained electronically, the CE must provide it in the form and format requested by the individual if readily producible, or if not, in a readable electronic form and format as agreed to by the CE and the individual.
- Fees limited by HIPAA and state law.

Request for Amendment

- Individual's have right to request amendment of PHI maintained in a Designated Record Set.
- CE can deny request for certain reasons, including if the PHI is accurate and complete.

Request for Restrictions

- Privacy Rule requires CEs to permit individuals to request a restriction on the use or disclosure of PHI.

- CE must agree to a request to restrict disclosures of PHI to a health plan if:
  - The disclosure is for purposes of payment or health care operations, and is not otherwise required by law; and
  - The PHI pertains solely to the health care items or services the individual paid for out-of-pocket in full.

- Should use some method to flag or make a notation in the record to identify restricted PHI.

Request for Confidential Communications

- CE health care providers must accommodate reasonable requests to receive communications of PHI by alternative means or at alternative locations.
- Cannot require explanation for reason of request.
- Can condition on:
  - Information as to how payment will be handled; and
  - Specification of an alterative address or contract method.

Request for Accounting of Disclosures

- Individuals have right to receive accounting of certain disclosures.

- Exceptions for disclosures:
  - For TPO
  - To the individual
  - Incident to another use or disclosure
  - Pursuant to an authorization
  - For facility directory or to family/friends when permitted by HIPAA
  - And others

Notice of Privacy Practices

- CE must inform patients how PHI about that patient will be used or disclosed.
- Lots of picky stuff has to be in there.
- Providers must give it to patient at first delivery of service and make good faith effort to obtain written acknowledgment of receipt.
- Every CE must post it on their website, if have one.

Business Associates/ Subcontractors

Workforce Member or Business Associate?

- There are some situations where a CE may treat a contractor as a member of its workforce (for purposes of HIPAA) instead of a BA – such as when a contractor provides services onsite and under the control of the CE.

- BUT – be careful to sort through the concepts of an independent contractor being deemed a member of the "workforce"…could have implications under tax and employment laws.

The BA Relationship Is Not Contingent On The BAA

- Having a BAA does not make everything you do compliant.
- Not having a BAA does not excuse you from liability if a BA relationship exists.
- A BA relationship exists if the person performing the services meets the definition of "business associate."
- This is true even if the parties fail to enter into a BAA – but then the failure is a HIPAA violation – for BOTH the CE and the BA.

"Oh we hardly see any PHI."

- Seeing a little PHI (or having the opportunity) is like being a little bit pregnant.
- The preamble to the Final Rule states that an entity is a BA even if the PHI it maintains is not diagnosis-specific and is not indicative of the health care services provided to the patient.
- Even if the only PHI that a BA receives is the fact that the patient received care or benefits from the CE, it must be protected by the BA in accordance with HIPAA.

Business Associate Obligations

- Business Associate Agreements (BAA) with subcontractors (and with CE).
- Policies/ Procedures.
- Breach Notification.
- Patient Rights (except NPP and Privacy Officer).
- Cannot de-identify PHI for its own use unless permitted by the terms of the BAA.
- DIRECTLY LIABLE, not just contractually.

Why Do We Care If A BA Is An Agent?

- (1) The CE is deemed to have knowledge of a breach at the same time as a BA if the BA is an agent.
  - CE has to notify patient of a breach within 60 days of when breach is known/ should have been known.
  - BA knowledge imputed to CE if BA is an agent.
- (2) The CE can be liable for BA HIPAA violations if the BA is an agent acting within scope of agency.

When Is A BA An Agent?

- Fact specific – analyzed under federal common law of agency.
- Depends overall on the right of the CE to control the BA's conduct.
- Can the CE give instructions/directions or does the contract give the BA the power to control its activities for the CE?
- Contract may be relevant but labels (e.g. "independent contractor") are not dispositive.

Breach Notification Rule

- Requires notification in the event of a breach of unsecured PHI (to patient and government, maybe the media).

- Breach means an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the PHI.
  - Subject to certain exceptions.

Breach Notification - Risk Assessment

- Now use an "objective" standard: Notification required unless a low probability that the PHI has been compromised.
  - Also, presumption that impermissible use or disclosure is a breach!
- Old "subjective" standard: Notification required if significant risk of financial, reputational, or other harm to the individual.
- Focus is now on the risk the PHI was compromised, instead of the risk of harm to the individual.

Four Factors to Consider

1. Nature and extent of the PHI, including types of identifiers and likelihood of re-identification.
2. Unauthorized person who used the PHI or to whom the PHI was disclosed.
3. Whether the PHI was actually acquired or viewed.
4. Extent the risk to the PHI has been mitigated.

Factor 1: Nature and Extent of the PHI

- Types of PHI involved
  - Financial Information:
    - Increased risk if sensitive financial information is involved (credit card numbers, social security numbers, or other information that increases the risk of identity theft or financial fraud).
  - Clinical Information:
    - Nature of the services (e.g., sensitive information such as menta health, STDs or AODA) → Not just sensitive information qualifies!
    - Amount of detailed clinical information involved (e.g., treatment plan, diagnosis, medication, medical history information, test results).
  - Minimum Necessary: Was it more than the minimum necessary amount?

Factor 2: Who Used or Received the Information

- Recipient's obligation to protect the privacy or security of the information.
  - Good: CEs, BAs, subcontractors or federal agencies.
  - Bad: Thieves, hackers.

- Recipient's ability to re-identify.
  - E.g., employer that receives dates of service and diagnosis of certain employees may be able to re-identify based on other information available to employer, such as dates of absence from work.

Factor 3: PHI Acquired/Viewed vs. Simply Exposed

- Determine whether the PHI was actually acquired or viewed, or whether there was only an opportunity for the information to be acquired or viewed.

PHI Disclosed	HHS Says
Laptop lost or stolen and later recovered, and forensic analysis shows that the PHI on it was never accessed	Could determine PHI was not actually acquired/viewed
PHI mailed to wrong individual, who opens the envelope and calls to report information received in error	Individual acquired/viewed the PHI

Factor 4: Extent the Risk Was Mitigated

- Quickly mitigating any risk to PHI that was improperly used or disclosed may lower the risk that the use or disclosure will constitute a breach.
  - E.g., receive assurances (e.g., a confidentiality agreement) from recipient that the PHI will be destroyed or will not be further used or disclosed.

- Consider extent and efficacy of the mitigation.
  - Assurances from employee, affiliated entity, BA, or other CE vs. assurances from other third parties.

Burden of Proof

- CE or BA has burden of proof for showing why breach notification was not required!

Notification Of The Patient

- Notice to the patient – mailing or (if patient has agreed) emailing.
- Substitute notice, if contact information out of date for:
  - Less than 10 patients: alternative written, phone, etc.
  - 10+ patients: posting on website for 90 days or notice in print or broadcast media.

Notification Of The Government

- FEWER THAN 500 PATIENTS: Enter logged breaches by 60 days after Jan. 1 of year in which breach is discovered.
- 500 OR MORE PATIENTS: Not later than 60 days following a breach.
- Submitted on OCR's website.

Notification of The Media

- If 500 or more people in a single state or "jurisdiction," notifying media is required.
- Prominent media outlets serving that community.
- Usually in the form of a press release.
- No later than 60 days after discovery of a breach.

Notification By A Business Associate

- If BA has a breach of CE PHI, BA must notify the CE.
- Without unreasonable delay and no later than 60 days from the discovery of the breach – OR WHATEVER IT SAYS IN THE BAA.
- CE then has 60 days to notify the patient UNLESS BA IS AN AGENT – then the 60 days runs concurrently.

HIPAA Enforcement

- Used to be complaint driven only – now affirmative audits.
- Penalties used to be mostly theoretical – now being imposed.
- State Attorney Generals can get in on the action.
- Whistleblowers can get a piece of the penalty in certain circumstances.

HIPAA Violation	Minimum Penalty	Maximum Penalty
Individual did not know (and by exercising reasonable diligence would not have known) that he/she violated HIPAA	$100 per violation, with an annual maximum of $25,000 for repeat violations (Note: maximum that can be imposed by State Attorneys General regardless of the type of violation)	$50,000 per violation, with an annual maximum of $1.5 million
HIPAA violation due to reasonable cause and not due to willful neglect	$1,000 per violation, with an annual maximum of $100,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million
HIPAA violation due to willful neglect but violation is corrected within the required time period	$10,000 per violation, with an annual maximum of $250,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million
HIPAA violation is due to willful neglect and is not corrected	$50,000 per violation, with an annual maximum of $1.5 million	$50,000 per violation, with an annual maximum of $1.5 million

Disclosures for Workers' Compensation Purposes

45 CFR 164.512(l) (Download a copy in PDF - PDF)

Background

The HIPAA Privacy Rule does not apply to entities that are either workers' compensation insurers, workers' compensation administrative agencies, or employers, except to the extent they may otherwise be covered entities. However, these entities need access to the health information of individuals who are injured on the job or who have a work-related illness to process or adjudicate claims, or to coordinate care under workers' compensation systems. Generally, this health information is obtained from health care providers who treat these individuals and who may be covered by the Privacy Rule. The Privacy Rule recognizes the legitimate need of insurers and other entities involved in the workers' compensation systems to have access to individuals' health information as authorized by State or other law. Due to the significant variability among such laws, the Privacy Rule permits disclosures of health information for workers' compensation purposes in a number of different ways.

How the Rule Works

Disclosures Without Individual Authorization. The Privacy Rule permits covered entities to disclose protected health information to workers' compensation insurers, State administrators, employers, and other persons or entities involved in workers' compensation systems, without the individual's authorization:

- As authorized by and to the extent necessary to comply with laws relating to workers' compensation or similar programs established by law that provide benefits for work-related injuries or illness without regard to fault. This includes programs established by the Black Lung Benefits Act, the Federal Employees' Compensation Act, the Longshore and Harbor Workers' Compensation Act, and the Energy Employees' Occupational Illness Compensation Program Act. See 45 CFR 164.512(l).

- To the extent the disclosure is required by State or other law. The disclosure must comply with and be limited to what the law requires. See 45 CFR 164.512(a).

- For purposes of obtaining payment for any health care provided to the injured or ill worker. See 45 CFR 164.502(a)(1)(ii) and the definition of "payment" at 45 CFR 164.501.

Disclosures With Individual Authorization. In addition, covered entities may disclose protected health information to workers' compensation insurers and others involved in workers' compensation systems where the individual has provided his or her authorization for the release of the information to the entity. The authorization must contain the elements and otherwise meet the requirements specified at 45 CFR 164.508.

Minimum Necessary. Covered entities are required reasonably to limit the amount of protected health information disclosed under 45 CFR 164.512(l) to the minimum necessary to accomplish the workers' compensation purpose. Under this requirement, protected health information may be shared for such purposes to the full extent authorized by State or other law. In addition, covered entities are required reasonably to limit the amount of protected health information disclosed for payment purposes to the minimum necessary.

Covered entities are permitted to disclose the amount and types of protected health information that are necessary to obtain payment for health care provided to an injured or ill worker. Where a covered entity routinely makes disclosures for workers' compensation purposes under 45 CFR 164.512(l) or for payment purposes, the covered entity may develop standard protocols as part of its minimum necessary policies and procedures that address the type and amount of protected health information to be disclosed for such purposes.

Where protected health information is requested by a State workers' compensation or other public official, covered entities are permitted to reasonably rely on the official's representations that the information requested is the minimum necessary for the intended purpose. See 45 CFR 164.514(d)(3)(iii)(A). Covered entities are not required to make a minimum necessary determination when disclosing protected health information as required by State or other law, or pursuant to the individual's authorization. See 45 CFR 164.502(b). The Department will actively monitor the effects of the Privacy Rule, and in particular, the minimum necessary standard, on the workers' compensation systems and consider proposing modifications, where appropriate, to ensure that the Rule does not have any unintended negative effects that disturb these systems.

PRESENTATION BY: Paige Fulton

Clean CLAIM MD

WORKING HARD SO YOU GET PAID

www.cleanclaimmd.com