HIPAA 101

Privacy & Security Overview

Compliance and Privacy
504-842-9323 | compliance@ochsner.org

Ochsner Health System

2019

Key Terms

Covered Entity (CE)	• A health plan, health care clearinghouse, or health care provider that transmits information electronically in connection with a covered transaction
Affiliated Covered Entity (ACE)	• Legally separate covered entities that are affiliated who designate themselves as an ACE for purposes of compliance with HIPAA if all of the CE's are under common ownership or control
Organized Healthcare Arrangement (OHCA)	• Arrangements that involve clinical or operational integration among legally separated covered entities in which the sharing of PHI is necessary for the joint management of the enterprise
Business Associate (BA)	• A party who receives protected health information to perform a service for the Covered Entity

Ochsner™ Health System

Key Terms

Protected Health Information (PHI)	• Individually identifiable health information about the past, present, or future treatment of a patient or the payment for that treatment. Includes name, MRN, full-face photos, etc.
Notice of Privacy Practice (NPP)	• Describes to the patient the uses and disclosures of PHI that may be made by the covered entity
De-identified Data	• Information that does not identify the individual and there is no reasonable basis to believe that the information can identify the individual (*not PHI so not protected under HIPAA)
Limited Data Set	• De-identified data that retains more detailed geographic information and dates of service. This **may** be shared under a Data Use Agreement.

Ochsner™ Health System

HIPAA Privacy- General Rule

- A covered entity may not **use or disclose** protected health information, except as permitted or required.
  - **Use**: Sharing, employment, application, utilization, examination, or analysis of individually identifiable health information within an entity that maintains such information
  - **Disclose**: Release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information

Ochsner™ Health System

Uses and Disclosures Required by Law

- There are 2 Mandatory Disclosures:
  - To the patient with some exceptions
  - To the Secretary of DHHS to investigate an alleged privacy violation

There are numerous scenarios where the disclosure of patient health information is permitted, some of which are listed on the next slide.

Ochsner™ Health System

Permitted Uses and Disclosures

- Permitted uses and disclosures include:
  - To the individual
  - For treatment, payment, and operations
  - In the event of an incidental disclosure
  - For disclosures to family and other caregivers, provided the individual has been given the opportunity to opt out
  - For public health purposes, law enforcement, and other limited purposes
  - For limited data sets
  - For other purposes pursuant to a valid authorization signed by the individual
  - To a Business Associate as permitted by a signed business associate agreement outlining the terms of the use and/or disclosure

Ochsner™ Health System

Ask yourself: Is using or disclosing this patient information in the best interest of the patient?

Impermissible Uses and Disclosures

- If an employee impermissibly accesses, uses, or discloses patient information, the covered entity has the duty to mitigate any harmful effects, impose sanctions (if necessary), and account for the disclosure or notify the patient of the breach.

- The covered entity has **60 days** from the date of notification to investigate the potential breach and notify the patient if necessary.

Ochsner™ Health System

Authorization Required

- All uses and disclosures of PHI that are NOT explicitly required or allowed under the regulations may only be done with an **authorization**.

- Examples:
  - Marketing
  - Research
  - Fundraising
  - Publishing

Ochsner™ Health System

Incidental disclosures

- Incidental disclosures are a secondary use or disclosure that cannot reasonably be prevented, is limited in nature, and that occurs as a result of another use or disclosure that is permitted by the Rule.
- These include a patient overhearing you discuss another patient's care in a shared treatment area, among others.
- As long as the covered entity uses **reasonable safeguards** to prevent incidental disclosures from occurring, they are permitted under the HIPAA privacy rule (but they often upset patients and family members)

Ochsner™ Health System

Scenario 1

You are in a crowded area and need to have an urgent discussion with a patient or her caregiver and a private room is not available.

What are some reasonable safeguards you can use to help lessen the chances of an incidental disclosure?

Ochsner™ Health System

Scenario 1

- It is always best to try to find a private area, with a door, away from others, to have patient care discussions, however, the HIPAA privacy rule acknowledges that it is not always feasible.
- The HIPAA privacy rule allows for reasonable safeguards, such as lowering ones voice when speaking, using a curtained off area or area with a partition, speaking in a room with a tv at volume.

Ochsner™ Health System

Reasonable safeguards

- The HIPAA Privacy Rule requires only that covered entities implement reasonable safeguards to limit incidental uses or disclosures.
- The Privacy Rule does not define reasonable safeguards, but standards have been developed in practice.
- Reasonable safeguards include measures, including but not limited to, curtain partitions, lowering of voices, televisions or music at volume, posting signage regarding confidentiality, and other technical measures that promote patient privacy.

Ochsner™
Health System

Communicating with patients, family, and caregivers

- If possible, seek a private area to speak with patients or others involved in patient care.
- If privacy is not available, ask the patient if they are okay with you discussing care in a non-private area.
- Ask patient if they are comfortable having family and guests present for care-related conversations.

Ochsner™ Health System

Minimum Necessary Rule

- Minimum Necessary is the core principle behind the HIPAA Privacy Regulation.

> *For all uses and disclosures of patient information, the **"minimum necessary rule"** should be followed – access, use, or disclose what you need and **only** what you need to do your job.*

- When accessing patient information, ask yourself:
  - Do I have permission to access this information?
  - Do I need this information to perform my job?
  - What exact information do I need to perform my job?
  - Does my co-worker need to know this information? Should I discuss it with them?

Ochsner™ Health System

Patients' Individual Rights

- Patients are given certain rights with respect to their health information:
  - Receipt of the Notice of Privacy Practices
  - Access to their health information
  - Ability to amend their health information
  - Request for confidential communications
  - Receive an accounting of disclosures of their PHI
  - Restrict how the covered entity may use or disclose their PHI

Ochsner™ Health System

Notice of Privacy Practices

- Patients have a right to receive the Notice of Privacy Practices (“NPP”) at their first encounter with the covered entity, and upon request.
  - CE must post NPP at the physical delivery site.
  - CE must make best efforts to receive acknowledgement from the individual about receipt of the NPP.
  - CE is bound by the terms of its NPP.

Ochsner™ Health System

Right to access health information

- The Privacy Rule generally requires HIPAA covered entities to provide individuals, upon request, with access to the protected health information (PHI) about them in one or more “designated record sets” maintained by or for the covered entity. This includes the right to inspect or obtain a copy, or both, of the PHI, as well as to direct the covered entity to transmit a copy to a designated person or entity of the individual’s choice.
- The designated record set does **not** include psychotherapy notes or information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.

Ochsner™ Health System

Scenario 2

A patient contacts your office stating that documentation in a note you completed is incorrect and wants the documentation changed.

What can be done in this situation

Ochsner Health System

Scenario 2

- In this case, the patient appears to be requesting an amendment, one of a patient's rights under HIPAA.
- All amendment requests that pertain to documentation prepared by the covered entity must be reviewed by the author and then the record must be updated if the reviewer agrees with the amendment or denied if the reviewer does not agree and a letter communicating the outcome must be sent to the patient.
- The HIPAA privacy rule sets a timeline of 60 days, with one 30 day extension for this process.

Ochsner™ Health System

Right to amend health information

- Patients have the right to request a change or amendment to their medical record if they think information in their medical or billing record is incorrect.
- The healthcare provider must respond to the request, and if the information is incorrect and the provider created the information, it must amend incomplete or inaccurate information.
- If the provider does not agree to the patient's request, the patient can submit a statement of disagreement that must be added to the patient's medical record.

Ochsner™ Health System

Right to request confidential communications

- Pursuant to HIPAA, patients may request that a covered entity contact them by alternative means.
- The covered entity must accommodate all reasonable requests.
- A covered entity may not require an explanation from the patient for why these alternative communication routes are needed.

Ochsner™ Health System

HIPAA Security

- The Security Regulation is designed to protect patient health information in ***electronic*** format (“ePHI”).

- The Security Rule requires that Ochsner meet four security objectives:
  1. Ensure the confidentiality, integrity, and availability of all electronic health information in their possession (CIA)
  2. Protect against any reasonably anticipated threats or hazards
  3. Protect against any reasonably anticipated impermissible access, use of disclosure of health information
  4. Ensure compliance with the Security Regulation by employees

Ochsner™ Health System

Email, Faxes & HIPAA

- If you do need to send PHI to an external recipient, it's best to communicate via telephone rather than email if you are unsure!
- Faxing- be sure that you have the recipient's correct information. Always use a coversheet with your contact information so that recipients can contact you if the fax goes astray.
- It is best not to text PHI, as texts are not always encrypted (check with your cellular carrier). There are secure texting platforms available, however; which may be used.

Ochsner™ Health System

Paperwork…

- Most of the breaches that compliance handles involve patient paperwork
  - If you see patient paperwork left unattended or in clear view, ask the employee to flip it over, secure it, or to shred it if no longer needed
  - Always double check the names on paperwork before giving it out to patients

Ochsner™ Health System

Scenario 3

You have reason to believe that patient information has been accessed by someone without authorization.

What should you do?

Ochsner™ Health System

Scenario 3

- If you suspect that a breach has occurred, notify your compliance department immediately.
- Your compliance department will begin an internal investigation to determine the cause of the breach and what can be done to mitigate the breach.
- Once the cause has been determined, your compliance department will notify the patient(s) involved and will work to remediate the incident, using education, training, progressive discipline and other methods in accordance with your institution’s sanctions policy.

Ochsner™ Health System

Breach Notification Requirements

- A **breach** is
  1) An unauthorized acquisition, access, use or disclosure of
  2) Unsecured PHI which
  3) Compromises the privacy or security of the PHI

  - A breach is presumed to be reportable unless there is a **low probability of compromise.**

In other words, it's a breach unless the CE can prove otherwise.

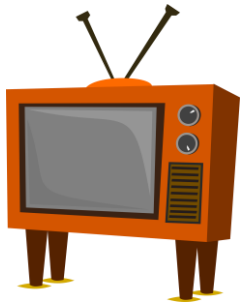
Ochsner™ Health System

Individual Breach Notification

- ≤ 500 individuals affected
  - Written form sent via first class mail
    - Can be sent via e-mail if the patient agreed to electronic notice
  - No unreasonable delay
  - Insufficient or out-of-date contact information for 10+ individuals obligates CE to provide substitute individual notice

- 500+ residents of a particular state or jurisdiction
  - Press release to prominent media outlet
  - No unreasonable delay

Ochsner™ Health System



Notice to the HHS Secretary

- In addition to notifying affected individuals and the media (where appropriate), CEs must notify the Secretary of the Department of Health & Human Services (HHS) of breaches of unsecured protected health information

  - Timeline for HHS Notification
    - If the breach involved <500 individuals, no later than 60 days after the calendar year in which the breach was discovered
    - If a breach affects **500+ individuals**, notice must be provided **without unreasonable delay** and in no case later than 60 days from discovery of the breach

Ochsner™ Health System

HIPAA Hints

- PHI and ePHI must be kept private and secure
- Only discuss information for work purposes
- Think before you share PHI verbally
- Only access the minimum PHI necessary to get your work done
- Log off when you leave your computer
- Use shred bins to dispose paperwork containing PHI
- Don’t share your computer password
- PHI must be protected when it travels
- Know when to call for HIPAA help-don’t guess when you are unsure how to handle a situation in a HIPAA complaint fashion

Ochsner™ Health System

Compliance & Privacy

Contact Info

504-842-9323 Main | compliance@ochsner.org

Anonymous Compliance Line

Toll Free 888-273-8442

Ochsner™ Health System