Table of Contents

How does the HIPAA Privacy Rule affect my relationship with my patients?

HIPAA does not change our ability to provide the highest quality health care. The Privacy Rule does not prevent physicians from discussing patient information with fellow providers for treatment purposes or prevent physicians from sharing information with family members caring for a patient. HIPAA does, however, change the way we think of who controls patient information. Under HIPAA, the patient is given more authority over their health information and how it is shared for purposes other than treatment.

USE AND DISCLOSURE OF PHI

For detailed information, see Policy 5031

Is a signed authorization always required to release PHI?

In general, a signed authorization is not required when doctors, nurses, therapists, dieticians, and others use or disclose information about patients to determine what services they should receive, to inform referring physicians or family members caring for a patient, when reviewing the quality of their care, or when billing for their services. HIPAA allows disclosure of PHI without authorization for certain defined purposes such as public health reporting, abuse and neglect reporting, or to researchers with an IRB approved waiver of authorization.

For a complete list, see Procedure 5031, Authorization Requirements for Use and Disclosure of Protected Health Information.

Can I leave a message for a patient on either their home phone or with a family member?

The HIPAA Privacy Rule permits providers to communicate with patients regarding their care. This includes communicating with patients at their homes, whether through the mail, by phone or in some other manner such as leaving a message on an answering machine. In addition, the Privacy Rule permits covered entities to disclose limited information to family members, friends, or other persons regarding the patient's care, even when the patient is not present. However, covered entities should use professional judgment to assure that such disclosures are in the best interest of the patient and limit the information disclosed.

When a patient has requested that the covered entity communicate with them in a confidential manner, the covered entity must accommodate that request, if reasonable.
For example, requesting that all correspondence be sent to a post office box rather than a home address or to receive calls at another phone other than their home phone are reasonable requests, absent extenuating circumstances.

Are there special requirements for use and disclosure of mental health information, HIV/AIDS related information or substance abuse treatment information?

PHI that contains mental health information, HIV/AIDS related information or substance abuse treatment information is afforded special protections under state and federal law distinct from HIPAA.

Connecticut State Law mandates that HIV/AIDS and mental health information not be released without written patient authorization which specifically indicates patient authorization to release this information. Federal regulations similarly require separate authorization for substance abuse information. Mental Health information must also be labeled as protected under state statute.

Without specific authorization to release HIV/AIDS, mental health, or substance abuse information, records must be redacted of any related information.

The Yale Authorization for Use and Disclosure of Protected Health Information form includes a separate section to obtain authorization and the additional signature needed when such records will be released.

Are there special requirements for psychotherapy notes?

Psychotherapy notes are defined as the notes of a mental health professional which document or analyze the contents of a counseling session and which are stored separately from the rest of the medical record. Because of their potential sensitivity, psychotherapy notes receive stronger protection. Except in limited circumstances, use or disclosure of psychotherapy notes is permissible only if the patient signs a separate authorization that encompasses *only psychotherapy notes*.

The Yale Authorization for Use and Disclosure of Protected Health Information form includes a separate section to obtain authorization and the additional signature needed when such records will be released.

Can I report to the appropriate state or federal agencies in cases of abuse and neglect, medical device malfunctions, or communicable diseases?

Yes. HIPAA does not supersede state or federal laws such as those that require clinicians to report cases of child or elder abuse, certain communicable disease, certain injuries such as gunshot wounds or adverse event reporting.

Can I disclose PHI about decedents?

A provider may disclose PHI to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death or other duties required by law. PHI of a decedent may also be disclosed to a funeral director. These disclosures must be included in the accounting for disclosure log. See Policy 5003: Accounting for Disclosures.

A decedent's record may also be disclosed to the executor/executrix of the estate or, if there is no appointed executor/executrix, to the surviving spouse or next of kin.

Note that records related to individuals deceased for more than 50 years are excluded from the definition of PHI and hence are not subject to disclosure restrictions.

Is an authorization needed to use and disclose PHI for cadaver organs, eyes or tissue donation purposes?

An authorization is not needed to use or disclose PHI to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaver organs, eyes, or tissue for the purpose of facilitating donation and transplantation procedures.

Does the HIPAA Privacy Rule require a signed authorization to release PHI for workers' compensation purposes?

The HIPAA Privacy Rule permits Yale, as a covered entity, to disclose PHI without a signed patient 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. Any additional PHI held by Yale which is not related to workers' compensation injuries, should not be disclosed to a workers' compensation carrier unless a signed authorization has been obtained from the patient.

Do patients have the right under the HIPAA Privacy Rule to restrict PHI disclosures for workers' compensation purposes?

Under the HIPAA Privacy Rule, patients cannot request that Yale restrict a disclosure of PHI for workers' compensation purposes if the disclosure is required by, authorized by, and necessary to comply with workers' compensation law or similar law.

Does an attorney request for PHI need an authorization?

An attorney request for disclosure of PHI can be honored when accompanied by an authorization signed by the patient or the patient's Personal Representative, or a court order directing disclosure to the specific named attorney. Subpoenas without a patient's authorization may also be honored if the attorney provides certification that the patient has received adequate notification. The HIPAA Privacy Office has appropriate forms which can be used to obtain certification and can assist with this requirement.

If PHI is disclosed in response to a subpoena or court order, only PHI expressly authorized by the court may be disclosed.

Subpoena should be forwarded to the Office of the General Counsel for review prior to any release of PHI.

Can PHI be reported to law enforcement without an authorization?

The HIPAA privacy rule permits covered entities to disclose PHI to law enforcement officials without a signed authorization under specific circumstances, most notably when a crime is committed at the University. There are other limited circumstances in which law enforcement can request limited information. Such requests should be forwarded to the HIPAA Privacy Office for review.

Can I provide information to a patient's family member or friend?

Usually yes. HIPAA allows information to be shared with individuals who are involved in a patient's care, unless the patient objects. When a family member or friend escorts a patient for an appointment, it is safe to assume that it is ok to provide information related to that visit to the family member or friend, especially as relates to providing care. For example, the family member or friend may need to know what symptoms would necessitate clinical follow-up. However if you are not sure if an individual present with the patient is involved in caring for the patient, you should ask for confirmation from the patient prior to discussing the patient's condition in front of that individual.

It is more difficult to determine whether or not to respond to phone calls from family members or friends. In some cases, you may be aware that a certain family member is handling the patient's care and questions from that family member could be answered. In other cases, it may be wise to ask for confirmation from the patient before providing information, although HIPAA does allow for a clinician to respond based on his/her professional judgment as to whether or not such a disclosure is appropriate.

Which parent is authorized to access a child's PHI when the parents are divorced?

Unless a parent has had their parental rights revoked through court actions, both parents continue to serve as the child's personal representative under HIPAA.

Do patients need to be informed of who has had access to their records?

HIPAA requires that, upon request, patients be provided with a listing of individuals external to Yale who have had access to or been provided a copy of their records for reasons other than treatment, payment, healthcare operations or without the patient's authorization.
Research records themselves are also subject to the accounting requirement when study PHI is:

- ☐ accessed for secondary data analysis by another researcher
- ☐ accessed by additional researchers or entities not included in the authorization form signed by the subject
- ☐ disclosed in unanticipated events such as theft or loss of records

Accounting logs must be maintained by the medical record personnel responsible for the record or may be submitted to the HIPAA Privacy Office.
For detailed information see HIPAA Policy 5003.

Does the "minimum necessary standard" apply to the medical staff?

Medical staff must make a reasonable effort to disclose or use only the minimum necessary amount of PHI in order to do their jobs. Making "minimum necessary" determinations is a balancing act for medial staff. Providers must weigh the need to protect patients' privacy against the appropriateness of the requested disclosure. For disclosures related to treatment or disclosure to the patient, minimum

necessary does not apply. Requests for PHI for research, payment, audits or other non-treatment purposes should be limited to only that information which is necessary for the requested purpose.

Access to PHI is audited and inappropriate or unauthorized access will result in disciplinary action up to and including termination.

For detailed information see HIPAA Policy 5037.

What if I see information that I do not need?

There likely will be occasions when you have access to confidential patient information that you do not need for your work. You must keep this information confidential and not use it in any way or disclose it to anyone, including coworkers, other patients, patient visitors or anyone else who may ask. This also includes blogging, instant messaging and text messaging.

What can I do to protect a patient's privacy?

The privacy and security of Yale's health information are critical priorities of the University.

Some common ways that clinical staff can protect patient privacy are:

- ☐ Be aware of your surroundings and lower your voice or if possible avoid conversations regarding patients in the elevator, cafeteria, or hallway
- ☐ Be cautious when dictating notes, especially in open clinic areas
- ☐ Close patient room doors and curtains in semi-private rooms when discussing treatments and administering procedures
- ☐ Do not leave messages on answering machines regarding patient conditions or test results
- ☐ Avoid paging patients using identifiable information that could reveal their health issue
- ☐ Do not leave patient information in any form unattended
- ☐ Do not discuss patients in an identifiable way

For additional information see: http://hipaa.yale.edu

Are there HIPAA Security requirements for electronic PHI (ePHI)?

The HIPAA Security Rule requires institutions and individuals to take appropriate steps to secure the integrity, availability, and confidentiality of electronic PHI (ePHI). ePHI is defined as any PHI that is created, stored, accessed or transmitted electronically.

Security requirements can change frequently and the web site should be referred to for the most recent policies and best practice guidelines.

The specific requirements for complying with the Security Rule can be found at: http://hipaa.yale.edu/security.

Is it ever permissible for staff to share passwords?

Absolutely not. Yale uses the unique net-id issued to each employee, faculty, staff, student or volunteer coupled with their user defined passwords to audit and monitor access to electronic systems. When employees have completed any required training courses they are given access to specific electronic functions needed to fulfill their job duties. Signing on with your net-id and personal password and allowing another person to use your access on any electronic system for **any** purpose is strictly forbidden and will result in disciplinary action up to and including termination.

For example, it would not be appropriate to sign on to Epic and allow any staff other than yourself, to schedule, change or cancel appointments under this one net id and password. Each staff member must sign on under their own net id and password.

When is the use of PHI in research permitted?

Research use of PHI is permitted under the Privacy Rule if any of the following conditions are met:

- ☐ An authorization is obtained from each individual in the study. This is in addition to the normal informed consent process required under the Common Rule.
- ☐ An IRB approves a request for a waiver of authorization.
- ☐ All health information is de-identified
- ☐ A "limited data set" (partially de-identified data) is used and a data use agreement is established with the organization providing the data.
- ☐ The data is used in a review preparatory to a research project, e.g., to develop a research protocol.
- ☐ The subjects are decedents.

For detailed information see HIPAA Policy 5032.

Additional detailed guidance on the requirements of HIPAA in the context of research is available in the *Researcher's Guide to HIPAA* at: http://hipaa.yale.edu.