Clinician's Guide to HIPAA Privacy

I. Introduction
- What is HIPAA?
- Health Information Privacy
- Protected Health Information

II. HIPAA's Impact On Clinical Practice, Treatment, Referrals And Payment
- How is PHI used?
- Reasons for Releasing PHI
- Psychotherapy Notes
- Using Information for Marketing Purposes
- Fundraising

III. Patient's Rights
- Notice of Privacy Practices
- Individual Right to Access and Amendment
- Designated Record Set
- Accounting for Disclosures
- Record Retention

IV. Operational Procedures for Protecting Privacy
- The "Minimum Necessary" standard
- Everyday Steps for Protecting Privacy
- What If You See Information You Do Not Need?
- Protecting Paper Records and X-Rays
- Security Considerations

V. Business Associates
- Who Are Business Associates?
- Disclosure of PHI Requires a Contract
- Monitoring Compliance by Business Associates

VI. Research
- When is the Use of PHI in Research Permitted?

VII. Resources and Links

# Clinician's Guide to HIPAA Privacy

## Introduction

### What is HIPAA?

HIPAA is the Health Insurance Portability and Accountability Act of 1996. HIPAA requires many things, including the standardization of electronic patient health, administrative and financial data. It also establishes security and privacy standards for the use and disclosure of "protected health information" (PHI).

The HIPAA Privacy Rule:

- Applies to health care providers and health plans. At Yale, the School of Medicine, School of Nursing, Psychology Department clinics and portions of the Benefits Office are required to comply with HIPAA and constitute the Yale Covered Entity;
- Establishes conditions under which PHI can be used and disclosed. Use of PHI refers to sharing the information within the Yale Covered Entity. Disclosure refers to sharing PHI to individuals or organizations outside of the Yale Covered Entity;
- Grants individuals certain rights regarding their PHI;
- Requires that we maintain the privacy and security of PHI.

The HIPAA Security Rule:

- Establishes administrative, technical and physical standards for the security of electronic health information;
- Requires that we maintain the availability, integrity, and confidentiality of electronic health information.

The American Recovery and Reinvestment Act (ARRA) and HIPAA

- The American Recovery and Reinvestment Act of 2009 includes legislation known as the Health Information Technology for Economic and Clinical Health (HITECH) Act which promotes the use of electronic health records (EHRs) by providing incentives to health care providers who convert their medical records from paper files to EHRs

This guide addresses the HIPAA Privacy Rule's requirements related to uses and disclosures of PHI as they relate to clinicians working at Yale. If you need further guidance on HIPAA or information related to the Security Rule, please refer to http://hipaa.yale.edu/

.

### Health Information Privacy

Privacy, according to the regulation, is an individual's right to control access and disclosure of their protected, individually identifiable health information. HIPAA requires that information provided by the patient to health care providers including notes and observations about the patient's health will not be used for purposes other than treatment, payment, health care operations or for the specific purposes described in the Privacy Rule.

The Privacy Rule does not prevent physicians from discussing patient information with fellow providers for treatment purposes. However, the regulations require providers to make a reasonable effort to disclose only that information which is necessary for securing payment and conducting standard health care operations such as audits and data collection.

## Protected Health Information

Protected Health Information (PHI) under HIPAA means any information that identifies an individual **and** relates to at least one of the following:

- The individual's past, present or future physical or mental health.
- The provision of health care to the individual.
- The past, present or future payment for health care.

Information is deemed to identify an individual if it includes either the individual's name or any other information that could enable someone to determine the individual's identity (e.g., address, age, Social Security number, e-mail address).

### Identifiers

Data are "individually identifiable" if they include **any** of the 18 types of identifiers, listed below, for an individual or for the individual's employer or family member, **or** if the provider or researcher is aware that the information could be used, either alone or in combination with other information, to identify an individual:

- Name
- Address (all geographic subdivisions smaller than state, including street address, city, county, ZIP code)
- All elements (except years) of dates related to an individual (including birth date, admission date, discharge date, date of death and exact age if over 89)
- Telephone numbers
- FAX number
- E-mail address
- Social Security number
- Medical record number
- Health plan beneficiary number
- Account number
- Certificate/license number
- Any vehicle or other device serial number
- Device identifiers or serial numbers
- Web URL
- Internet Protocol (IP) address numbers
- Finger or voice prints
- Photographic images
- Any other characteristic that could uniquely identify the individual

# HIPAA's Impact on Clinical Practice, Treatment, Referrals and Payment

## How is Protected Information Used?

Information that Yale collects or creates that relates to patient health or to patient care can only be used in limited ways without patient authorization.

Patient authorization is not required when doctors, nurses, therapists, dieticians, and others use information about patients to determine what services they should receive or to review the quality of their care. PHI may also be used without patient authorization to bill patients (or their insurance companies) for the services they received or to fulfill other necessary administrative and support functions.

Disclosure is also permitted without authorization in a number of other situations, such as where disclosures are required by law. Below is a list of some common situations where PHI can be released without a patient's authorization:

### Reasons for Releasing PHI

There are certain situations in which Yale may release PHI without the patient's authorization. These include:

- Providers are required to report certain communicable diseases to state health agencies, even if the patient doesn't want the information reported.
- The Food and Drug Administration requires that certain information be reported about medical devices that break or malfunction.
- The courts have the right to order providers to release patient information with appropriate certifications or court orders.
- Under limited circumstances, health care providers may disclose PHI to police (such as reporting certain wounds or injuries, or to comply with a court-ordered warrant or grand jury subpoena).
- When physicians or other people providing patient care suspect child abuse or elder abuse, they must report it to state agencies.
- The hospital or provider reports information to coroners and funeral directors in cases where patients die.

Patients can also request release of their information by signing an authorization which includes all the statements required under the regulations. Use of the Yale University Authorization for Use and Disclosure of PHI (form 5031) meets the regulatory requirements. When responding to an authorization from another organization for release of protected health information, the authorization must also meet the HIPAA requirements. If there is any doubt, the Privacy Office can provide assistance in reviewing the validity of the document.

## Psychotherapy Notes

Psychotherapy notes receive stronger protection than other protected health information under the HIPAA privacy rule because of their potential sensitivity. 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. Except in certain limited circumstances, use or disclosure of psychotherapy notes is permissible only if the patient signs a separate authorization that encompasses *only psychotherapy notes* and no other PHI.

Psychotherapy notes exclude:

- Medication prescription and monitoring
- Counseling session start and stop times
- Modalities and frequencies of treatment furnished
- Results of clinical tests
- Any summary of diagnosis, functional status, treatment plan, symptoms, prognosis, or progress to date

### Using Information for Marketing Purposes

Yale can continue to communicate with our patients concerning the health care services we provide without obtaining patient authorization. For example, a clinical department may describe the health care services it offers, or a clinician may recommend treatments, therapies or other health care providers in the course of treating a patient. Similarly, a marketing authorization is not needed to inform patients of a new service or health care program or of a change in office location.

However, the HIPAA privacy rule does not allow us to disclose PHI to another organization for that organization's marketing purposes unless the patient authorizes that disclosure.

### Fundraising

Yale may use limited protected health information for its own fundraising efforts (demographics and dates of services only). Demographic information includes names, addresses and other contact information, age, gender, and insurance status.

For example, a healthcare facility wants to build a heart center and runs a fundraising campaign. The privacy regulations allow the facility to use the names of people who have been seen within the past five years to send these individuals fundraising information.

Yale may solicit donations by mail. All fundraising communications must offer the individual the chance to opt out of receiving any further fundraising communications. If someone opts out, we must make reasonable efforts to honor that request.

## Patient's Rights

### Notice of Privacy Practices

The Notice of Privacy Practices (NOPP):

- Explains privacy policies
- Explains how patient information will be used
- Informs patients about their rights

Who receives the NOPP?

- First time patients
- Research subjects in a study that is also providing clinical care
- Anyone who requests a copy

Patients must be asked to sign an acknowledgement of receipt, although they are not required to sign it. The NOPP must be posted prominently in patient areas.

## Individual Right to Access and Amendment

Patients have a right to inspect and copy their health information that is maintained in their designated record set (definition below). The patient is required to either write a letter or fill out a form to request access. Patients can also request amendments to their medical records. Note that Yale staff who are also Yale patients must also follow this procedure to access their own records.

Exceptions to this rule:

- Certain types of research studies (e.g., those that use blinding)
- If the access could endanger the patient or others

## Designated Record Set

A designated record set is comprised of the following documents which are part of the patient's permanent medical record:

- Identification Sheet/Face Sheet
- Advance Directives
- Problem List
- History and Physical
- Progress Notes (including interdisciplinary documentation)
- Consultations
- Diagnostic Imaging Reports
- Laboratory Reports
- EKG Reports
- EEG Reports
- Pathology Reports
- Reports of Operations/Procedures
- Therapy Reports
- Graphic Sheets
- Medication Records
- Nursing Documentation
- Immunization Records
- Discharge Instructions
- Consents and Authorizations

- Home Health Documentation
- Photographs (if included in the medical record)
- Medical Release Forms
- Requests for Amendment
- Amendments
- Denials of Requests for Amendments

The following documents that are part of billing records retained for patients are also included in the designated record set.

- Life Time Insurance Authorization (LTIA) (scanned image)
- Medicare Advanced Beneficiary Notice
- Payment Agreement
- Requests for Amendment
- Amendments
- Denials of Requests for Amendments

### Accounting for Disclosures

HIPAA requires that, upon request, patients be provided with a listing of who has had access to or been provided a copy of their records (1) for reasons other than treatment, payment, healthcare operations - unless such disclosures are made from an electronic health record. or (2) without the patient's authorization. In order to meet this requirement, accounting logs must be maintained by the medical record personnel responsible for the record. The logs must include who had access, for what reason and when access was provided. This requirement also holds true for research access to PHI when access is granted under a waiver of authorization, for recruitment purposes or for research on decedents.

In an effort to minimize the burden on record holders and to comply with HIPAA's research use requirements, researchers may be asked to complete accounting logs for clinical departments or Yale-New Haven Hospital (YNHH). These logs may be stored with the records or in an electronic database.

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

## Operational Procedures for Protecting Privacy

### The "Minimum Necessary" Standard

Medical staff must make a reasonable effort to disclose or use only the minimum necessary amount of protected health information in order to do their jobs. They can disclose information requested by other health care providers if the information is necessary for treatment.

Physicians and providers who are directly involved in the care of the patient can see PHI. Providers can disclose to consulting physicians or for referrals, but not to people who don't have clinical responsibilities. Physicians must be careful about what they disclose to other staff members, such as billing department workers or providers not involved in the care of their patient.

Making "minimum necessary" determinations is a balancing act. Providers must weigh the need to protect patients' privacy against their reasonable ability to limit the information that is disclosed while delivering quality care.

At Yale New Haven Health System (YNHHS) facilities, inappropriate or unauthorized access will result in disciplinary action up to and including removal from the Medical Staff. YNHHS can audit access to PHI and monitor the use of electronic resources without an individual's knowledge, with the exception of phone conversations.

## Everyday Steps for Protecting Privacy

Here are some common ways that clinical staff members can protect patient privacy:

- Talk on the phone in closed quarters, and be careful what you disclose aloud
- Close patient room doors when discussing treatments and administering procedures. Close curtains and speak softly in semi-private rooms when discussing treatments and administering procedures.
- Avoid discussions about patients in elevators and cafeteria lines.
- Do not leave messages on answering machines regarding patient conditions or test results.
- Avoid paging patients using identifiable information, such as their condition, name of physician, or unit that could reveal their health issues.
- Avoid leaving a patient's medical file on your computer screen when you leave your desk. It is best to log off when leaving a workstation. In public areas, point computer monitors so that visitors or people walking by cannot view information.

## What If You See Information You Do Not Need?

There likely will be occasions when you will have access to confidential information that you don't need for your work. For example, if a patient is placed in an isolation room, you may become aware of why he or she is there, or may suspect you know why. This is confidential information about a patient; do not communicate it to anyone else. You may see patient information posted on whiteboards in restricted areas where the public cannot see them. You must keep this information confidential. Do not use it in any way, and do not disclose it to anyone, including coworkers, other patients, patient visitors, or anyone else who may ask. In the course of doing your job, you may find that patients speak to you about their condition. Remember that what they tell you is confidential.

## Protecting Paper Records and X-Rays

When patient information is in your possession, regardless of form, you are responsible for keeping it safeguarded. Do not leave it unattended in an area where others can see it. This is especially important in public buildings, provider locations, and areas with heavy pedestrian traffic.

When you are done using patient information, either paper or film, return it to its appropriate location, e.g., the medical records department or a file at a nursing station.

When discarding paper patient information, make sure the information is shredded. X-Rays may be placed in confidential receptacles, located in all clinical areas of YNHH that are designated for the disposal of medical information (i.e., PHI). Leaving patient information intact in a wastebasket can lead to a privacy breach.

## Security Considerations

HIPAA requires that the privacy of PHI be maintained by limiting its uses and disclosures and that reasonable steps are taken to ensure that PHI is secure. Most often, breeches of privacy can be traced to lax security, so the two issues are intimately related. In April 2005, a portion of HIPAA known as the Security Rule became effective. The 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. The Security Rule requirements apply to all electronic computing and communication systems that create, store, or transmit PHI, both on-campus and off-campus. All users must comply with the Yale IT Appropriate Use Policy. The specific requirements for complying with the Security Rule can be found at http://hipaa.yale.edu/security/

Security requirements can change frequently and the web site should be referred to for the most recent policies and best practice guidelines. Some general guidelines to secure data include:

- Access to paper files should be limited by locking file cabinets or locking rooms with files.
- All computers must be password protected by using the ITS best practices for creating strong passwords.
- PHI can not be transmitted using instant messaging or other insecure “Peer to Peer” software.
- Use of unencrypted e-mail to send PHI is limited in accordance HIPAA policy 5123 “Electronic Communication of Health Related Information.” However, e-mail is allowed within or between Yale and Yale-New Haven Hospital.
- Computing devices must be physically secured e.g., via use of locking cables for laptops or locking up storage devices such as memory sticks.
- Computing devices should be maintained with appropriate anti-virus and anti-spy ware software.
- Databases containing PHI may also need an additional level of password protection to restrict access to the database itself and may need to be assessed via the ePHI tracking system.
- All electronic computing and communication devices must be stripped of all PHI prior to disposal or re-use.
- Data should be routinely backed-up.
- Use secure network access procedures for connecting to the Yale network from off site locations.

## Record Retention

HIPAA related documentation must be maintained for 6 years. This requirement applies to accounting for disclosures records, authorizations, data use agreements and any other

HIPAA forms. Connecticut medical records law requires that medical records be maintained for 7 years.

## Business Associates

### Who Are Business Associates?

HIPAA defines business associates as entities outside of Yale that perform or assist Yale in performing activities that require the use or disclosure of PHI. The information includes claims processing, data analysis, billing, practice management, or re-pricing.

Business associates include lawyers, actuarial professionals, accountants, health care consultants, transcription agencies, computer support, and billing companies. If you have a contract with someone helping you to do your job, he or she probably qualifies as a business associate.

### Disclosure of PHI Requires a Contract

Individuals at Yale cannot disclose protected health information to business associates unless the two parties have a contract. If you think you have a business associate relationship, contact your departmental business office or the Procurement Office (procurement@yale.edu ).

Before an individual at Yale gives PHI to a business associate, a contract must be signed. The contract must contain certain assurances including:

- A confidentiality clause that holds the business associate accountable for protecting PHI.
- A statement that the business associate cannot use or further disclose the information in a manner that violates the Privacy Rule.
- A statement that the business associate must safeguard the information as if it were the covered entity under the law.
- A statement that the business associate will require any subcontracts involving Yale PHI will also be held to the same HIPAA standards.

At the termination of contracts, business associates must return or destroy all protected health information within a reasonable amount of time.

### Monitoring Compliance by Business Associates

Business associates are required to report any privacy breaches or security incidents to the Privacy Office. The Business Associate and Yale are obligated to take steps to mitigate the situation, which might include termination of the contract or reporting the business associate to the Secretary of the U.S. Department of Health and Human Services.

A good rule of thumb: Limit information provided to business associates to what's needed to do the job. If possible, provide de-identified data instead of patient-identifiable data.

## Research

## 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:

- Authorization is obtained from each individual in the study. This authorization 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.

The "Request for Access to PHI for Research Purposes" form indicates what supporting documentation or certifications are necessary to provide a research investigator with access to PHI. This form must be collected from the individual who wishes to make use of the records along with the IRB approval and other relevant documentation as outlined in the Request for Access form.

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

## HIPAA Contacts and Links

University HIPAA Privacy Office
2 Whitney Avenue, Suite 204
P.O. Box 208252
New Haven, CT 06520-8252
Phone: (203) 432-5919
Fax: (203) 432-4033
**http://hipaa.yale.edu/**
HIPAA Privacy Office/School of Medicine
P.O. Box 208252
New Haven, CT 06520-8252
Phone: (203) 436-3650
Fax: (203) 432-4033

Yale University HIPAA Web Site
includes both Privacy and Security Rule Information
**http://hipaa.yale.edu/**

U.S. Department of Health & Human Services, Office of Civil Rights, (OCR)
**http://www.hhs.gov/ocr/hipaa/privacy.html**

*This guidebook will be regularly updated. Please be sure to check the HIPAA website at the URL listed above for the most recent copy.*

**Visiting Clinician Certification**

**Compliance with HIPAA**

I understand that patient records including demographic, biographic, insurance, financial, and clinical information are confidential and are subject to the requirements of HIPAA. In the course of employment or association with Yale University, this type of confidential information may be required and consequently accessed from file folders, computer display screens, and computer printers. I understand that I should only access that information which I need to perform my work-related duties.

Release of this confidential information, either written or verbal, except as required in the performance of work, is a critical violation of employee conduct. As such, it may be considered reason for immediate termination and could result in civil and criminal penalties under the Health Insurance Portability and Accountability Act of 1996 as amended by the HITECH Act of 2009. I have read and understand the Visiting Clinician's Guide to HIPAA and agree to the above statements.

_____ _____

Signature Date

_____ _____

Please print or type name Home Institution/Physician Practice

_____

Yale Departmental Affiliation

**Forward to:**
HIPAA Privacy Office
2 Whitney Ave. Suite 204
P.O. Box 208252
New Haven, CT 06520-8252
Fax: 203-432-4033

Version 05/2010