Yale University

HIPAA PRIVACY

HIPAA PRIVACY FAQs

For a detailed explanation of HIPAA policies and procedures see: http://www.hipaa.yale.edu. The information provided here does not supersede or take the place of the official HIPAA policies and procedures. This is intended solely as a reference guide. Version August 2014

Yale University

HIPAA PRIVACY

Table of Contents

For a detailed explanation of HIPAA policies and procedures see: http://www.hipaa.yale.edu. The information provided here does not supersede or take the place of the official HIPAA policies and procedures. This is intended solely as a reference guide. Version August 2014

For a detailed explanation of HIPAA policies and procedures see: http://www.hipaa.yale.edu. The information provided here does not supersede or take the place of the official HIPAA policies and procedures. This is intended solely as a reference guide. Version August 2014

I. PRIVACY FUNDAMENTALS

What is HIPAA?

HIPAA stands for the Health Insurance Portability and Accountability Act which was passed into law by Congress in 1996. HIPAA includes requirements for ensuring that health information is kept private, establishes patient rights with regards to that information and creates standards for the protection of electronic health information.

HIPAA was designed with the goal of providing for increased access to health insurance and reducing health care costs by simplifying health insurance administration. The law in part promotes electronic transmission of standardized health insurance information. While this was expected to streamline health care administration, these large electronic data sets could also be misused. For example, computer databases can be used to easily identify individuals who have medical conditions which would require expensive care and that information could be used to hinder those patients' ability to obtain insurance coverage or employment. Public concern over privacy led Congress to include privacy and security requirements in HIPAA. These provisions were promulgated as the HIPAA Privacy Rule which went into effect April 14, 2003 and the HIPAA Security Rule that went into effect in April 2005.

Medical research institutions, health care organizations and health care providers have always voluntarily adopted and implemented professional practices to protect patient privacy. Under HIPAA, the obligation to ensure the privacy of patient information became federal law.

What is HITECH?

HITECH stands for the Health Information Technology for Economic and Clinical Health Act. HITECH included revisions to strengthen the HIPAA Privacy Rule, added breach notification and increased enforcement provisions. The changes included allowing patients to request electronic copies of their records, increasing accountability of business associates, and revising the authorization requirements for research uses. For a compete list of the changes see http://hipaa.yale.edu/resources/stay-current

Who needs to abide by HIPAA?

At Yale, all faculty, staff, trainees, students and others in or working in support of Yale's HIPAA Covered Components: the Schools of Medicine (excluding the School of Public Health, the Animal Resources Center, and the basic science departments: Cell Biology, Cellular and Molecular Physiology, Comparative Medicine, History of Medicine, Immunobiology, Microbial Pathogenesis, Molecular Biophysics & Biochemistry, Neurobiology, and Pharmacology) and Nursing, Yale Health, Department of Psychology clinics and the employee welfare benefit program (Benefits Office) are required to understand their responsibilities under HIPAA and adhere to Yale's HIPAA policies and procedures.

Are there penalties for not complying?

Protecting the privacy of health information is a major component of HIPAA. Civil and criminal penalties may be imposed by the Federal government for failure to comply with HIPAA, including up to a 10-year jail sentence and a fine of up to $1,500,000 per incident.

Within Yale we continuously monitor HIPAA compliance and follow up on concerns and complaints. In both cases, we may use audit reports of access to PHI contained in electronic systems, chart audits, site visits, interviews and file audits.

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

Employees who fail to follow HIPAA policies are subject to disciplinary action up to and including immediate termination of employment.

What is PHI?

PHI= Protected Health Information

PHI is the information that we must keep private under HIPAA.

PHI means any information that identifies an individual **and** relates to their health care including at least one of the following:

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

Note that patient names, in and of themselves, when derived from health care or payment for health care here are considered to be PHI and must be protected according to HIPAA.

What identifies an individual?

In addition to the obvious information such as the patient's name, Social Security number or medical record number, there are more obscure pieces of information that are considered identifiers under HIPAA such as date of birth, an internet protocol (IP) address, or the serial number on a medical device.

For a list of all identifiers see: http://hipaa.yale.edu/sites/default/files/files/5039-EX-De-ID-EXA.pdf

Whose records are covered by HIPAA?

HIPAA compliance covers the private health information of **EVERYONE.** Some of this information may relate to people you know: family members, coworkers, friends, acquaintances, members of clubs, churches or other organizations, neighbors, celebrities, etc. Remember HIPAA protection covers all of the private health information held in any form by the School of Medicine (excluding the School of Public Health, the Animal Resources Center, and the basic science departments: Cell Biology, Cellular and Molecular Physiology, Comparative Medicine, History of Medicine, Immunobiology, Microbial Pathogenesis, Molecular Biophysics & Biochemistry, Neurobiology, and Pharmacology), School of Nursing, Yale Health, Department of Psychology clinic, and the Benefits Office.

No one is left out!

Your job duties may lead you to come across information of people you know or you may have access to databases or files that would include people you know. If you do not need that information to do your job, you are violating HIPAA and Yale policy by looking at that information.

Note that some positions may require access beyond their immediate area in order to provide the best service to our patients. For example, an individual who schedules patient visits for one department may be asked by the patient to check upcoming visits to another department in the process of selecting an appropriate appointment time. Doing so is not absolutely necessary for scheduling the visit but is appropriate to maximize patient satisfaction and is allowable under HIPAA.

What if I am both a patient and an employee?

You may be both a staff member and a Yale patient. HIPAA policies do not prohibit you from accessing your own record. However, using your job related access to health information systems to access information of anyone else, including a person that you are legally authorized to represent such as your child, is not allowed unless you are doing so as part of your normal job functions. For example, if your role is to process payments and paperwork related to payment for services as part of your daily work, including services your child received, it is perfectly appropriate to process those claims.

What is meant by the "Minimum Necessary" Standard?

HIPAA requires that even after we limit access to those who need the information to perform their job functions, we need to further limit access to what is the "**minimum necessary**" information. Minimum necessary refers to only accessing or disclosing those pieces of the PHI which are needed for a given activity.

Good clinical practice may require physicians to review the entire chart to provide care to a patient, making the entire record the "minimum necessary" information. On the other hand, when an internal auditor is reviewing claims made in relation to a research study, only those visits related to the research study in question constitute the "minimum necessary" information.

Depending on your job, you may handle charts often, but only need to actually read parts of it to obtain the necessary information. For example, when searching for notes or additional information that is needed or requested by a carrier to submit with a claim for reimbursement, additional payment, an appeal, etc., you would only need to go to the section of the chart that pertains to that information and search for the date(s) of service. The same criteria would apply when searching for notes using electronic software on your computer.

Reading through the documentation just to see a patient's medical history would not only be unnecessary and inappropriate, it would be in violation of HIPAA. When you need to see patient information to do your job, remember that the information is private and you are not allowed to repeat it, disclose it or share it with others unless they also need the information to do their job.

Your responsibility to maintain patient privacy continues even when you no longer work for Yale.

When can PHI be used within Yale without a signed patient authorization?

Under HIPAA guidelines, PHI can be accessed and used within Yale without a written patient authorization in limited ways such as:

- To provide treatment to that patient.
- To verify that patients are receiving quality care.
- To review and process benefit claims, including claims under the University's Flexible Benefits Plan.
- To fulfill administrative requirements such as physician credentialing, auditing, or legal review.
- To fulfill Yale's educational requirements to train students in medical care and administration.

In summary, PHI may be accessed for the purposes of **T**reatment, **P**ayment and health care **O**perations (TPO) without a signed written authorization from a patient.

For a complete list of when you can access PHI without a signed patient authorization, see HIPAA Policy 5031 at http://hipaa.yale.edu/policies-procedures-forms

When can PHI be disclosed to others outside of Yale without a signed patient authorization?

Under HIPAA guidelines, PHI collected by a healthcare organization or health plan can be disclosed to others who are not part of Yale without a signed patient authorization in limited circumstances. Some examples are:

- To the patient themselves or their legal representative.
- To physicians involved in the patient's care such as a physician who refers a patient to Yale or to whom Yale refers a patient.
- To the patient's insurance carrier to pay for treatment Yale provides except in cases where the patient has paid in full and requests that the information not be disclosed to their insurer.
- To organizations acting on Yale's behalf when an appropriate signed agreement known as a Business Associate Agreement is in place.
- To researchers if they have obtained a waiver of authorization from the IRB (Human Investigation Committee or Human Subjects Committee).
- To report certain communicable diseases to public health agencies.
- To appropriate government authorities regarding victims of abuse, neglect or domestic violence.
- To workers' compensation carriers for reporting and billing purposes.
- To medical examiners and funeral directors on behalf of deceased patients.
- To facilitate the donation and transplantation of organs.

For a complete listing of when PHI can be disclosed see HIPAA Policy 5031 at http://hipaa.yale.edu/policies-procedures-forms

Who do I go to with questions or complaints?

HIPAA requires each organization to appoint a Privacy Officer to oversee privacy practices under HIPAA. At Yale, this person is one of the key staff members responsible for developing the organization's privacy policies, monitoring and enforcing compliance with the law and responding to questions and complaints.

Deputy Privacy Officers at Yale School of Medicine, Yale School of Nursing, Yale Health, the Department of Psychology, and the Benefits Office are available to respond to day-to-day privacy matters.

When you have questions about privacy policies and the protection of individual patient health information, consult Yale's HIPAA web site (http://hipaa.yale.edu) which provides access to Yale's policies, procedures and guidance relating to HIPAA.

You can reach the Privacy Office at hipaa@yale.edu or by phone at 432-5919.

Patient complaints of privacy violations should be addressed through the standard patient complaint procedures of the clinical unit. They may also be addressed to the University Privacy Officer or the appropriate Deputy Privacy Officers.

Staff members who know or have reason to believe that someone has violated Yale's policies regarding HIPAA should report the matter promptly to their supervisor or a Privacy Officer. Anyone who expresses concern in good faith is protected by federal law against retaliation and harassment as

a result of raising the concern. If there are concerns about possible retaliation or harassment they should be reported to the University Privacy Officer for further investigation and resolution.

If you have questions about the security of electronic PHI, you should contact Information Security at information.security@yale.edu.

How do I guard records?

Patient records should be stored so that:

- access is limited to those who need the records for legitimate purposes.
- paper files and films are stored in locked cabinets or in rooms that can be locked when staff is not around.
- electronic records are secure according to the requirements described in the HIPAA Security Rule.

For complete information about guarding electronic records go to the HIPAA Security Rule website at: http://www.hipaa.yale.edu/security.

Do not dispose of any type of records containing PHI in open receptacles or regular trash container. Paper records that are no longer needed must always be shredded or placed in closed receptacles for delivery to a recycling company that will shred them. Contact your supervisor if the receptacle is full and a replacement is needed.

Access to computers and databases containing PHI must be limited through good password protection.

Never leave a disk, flash drive or anything containing patient information unattended in an in-box, or on a desk chair in an unlocked area. Deliver materials and documents that contain PHI personally to ensure privacy and unnecessary disclosure.

Laptops and other portable computing devices are particularly susceptible to loss or theft and are required to be encrypted using University endorsed encryption software. Follow the guidance on both the HIPAA Privacy and HIPAA Security web sites.

Store all computer disks and flash drives in locked areas and avoid labels that draw attention to the file content. Computers and external storage media must be fully erased prior to being discarded or re-used. Fully removing data requires more than just deleting files from the computer. See http://its.yale.edu/secure-computing/protecting-yales-data/secure-removal-data-or-disposal-computing-devices for more information.

How do I protect faxes?

Faxed patient information can easily fall into the wrong hands, which would be a violation of privacy and possible be considered a breach requiring notification to the patient and the US Department of Health and Human Services.

Check that the correct number is dialed into the fax or program frequently used numbers.

If you receive a fax in error, contact the sender and shred the information.

If you send a fax to the wrong number, contact the recipient and request that the fax be securely destroyed and then contact the Privacy Office to report the unauthorized disclosure.

Do not let faxed patient information lie around a fax machine unattended. Immediately place the faxed information in a secure and private location.

Be sure to always use a fax cover sheet that includes the HIPAA confidentiality statement.

Here is an appropriate HIPAA fax **Confidentiality Statement** that must be included on all faxes:

> The documents accompanying this transmission may contain confidential information that is legally protected. This information is intended only for the use of the individual or entity named above. **If you are not the intended recipient**, you are hereby notified that any disclosure, copying, distribution, or action taken in reliance on the contents of these documents is strictly prohibited. If you have received this information in error, please notify the sender immediately by calling us or sending a return fax indicating that you have arranged for the return or performed destruction of these documents.

How do I protect e-mail?

Sending PHI via e-mail to non-Yale, non-YNHH addresses is strongly discouraged because of privacy concerns:

- The message usually travels on the Internet and is not secure from unauthorized access while in transit.
- Emails are easily misdirected to the wrong recipient or to a recipient whose identity can not easily be verified.

If you must send PHI via email outside of the yale.edu, ynhh.org, bpth.org, or Greenwichhospital.org domains, you must adhere to the guidelines at http://hipaa.yale.edu/faq/guidance-faq/guidance-use-email-containing-phi including use of a Yale managed device, limiting identifiers and sensitive information to an absolute minimum and include the e-mail Confidentiality Notice.

Here is the HIPAA **e-mail Confidentiality Notice** that must be included on all e-mail containing PHI:

Please be aware that e-mail communication can be intercepted in transmission or misdirected. Please consider communicating any sensitive information by telephone, fax, or mail. The information contained in this message may be privileged and confidential. If you are NOT the intended recipient, please notify the sender immediately with a copy to hipaa.security@yale.edu and destroy this message.

Are there requirements for passwords and computer security?

Passwords and other security features that control access to computer systems help to protect PHI. They also make it possible for Yale to monitor who gains access to health records to ensure that they are being used appropriately.

The following procedures help to prevent the misuse of passwords:

- Never share passwords, never let someone else use your password, and never log into the system using borrowed credentials (a password or any other authorization method).
- Choose a password to make it as difficult as possible for someone to make educated guesses about what you've chosen.
- Try to choose a password that you will remember and don't have to write down.
- If you do write your password down, keep it in a secure and private location. Do not post your password or keep it where others can easily find it.

Employees who use computerized records must not leave their computers logged in to the patient information system while they are not at their workstations. When not in use, computer screens containing patient information or access to patient information must be turned away from the view of the public or people passing by.

You can lock your computer screen whenever you leave your computer unattended or out of your view – simultaneously press the Ctrl, ALT, Delete keys and then chose "Lock Computer" tab. You will need to sign on with your password to gain access when you return.

For complete information on HIPAA Security refer to: http://hipaa.yale.edu/security

What are Some Quick Tips for Protecting Patient Privacy?

- Use good judgment in oral communications and avoid unnecessary discussions, sharing and gossiping about patient information.
- Conduct any discussions with patients, or about patients, regarding their financial or health information in a private area and keep the information confidential.

- Do not discuss or share any patient's financial or health information with anyone who does not need the information to do their job.
- Never access or disclose patient information for personal reasons or out of curiosity.
- Be aware of your voice level when discussing patient information either on the phone or in person.
- If you need to discuss patient information with a coworker to do your jobs, do so face to face in an appropriate place. Avoid "over the cube," elevator or curb-side discussions.
- Be aware that you may not know who is on the other side of the cube.
- Be aware of individuals who come into your work area.
- Do not leave patient medical records where others can easily see or access them.
- Turn pages containing patient information over so PHI is face down.
- Keep laboratory, radiology, and other ancillary test results private.
- Arrange your work area to avoid public or unauthorized staff from viewing patient information.
- Do not leave screens containing patient information open on your computer.
- Do not leave your computer unattended – either log off or set your computer to automatically lock with password protection when unattended or manually lock your computer when you leave your computer area.
- Do not share your ID or passwords with anyone – you are responsible for activities tracked on a computer when your password is used.
- Always use a fax cover sheet with the HIPAA confidentiality statement – for both internal and external faxes.
- Verify fax numbers to which information is being sent.
- Program frequently used numbers into the fax machine.
- Do not leave documents on fax or copier machines.
- Should you receive a fax in error be sure to contact the sender and shred the information.
- Access, print, send, fax or e-mail only the "Minimum Necessary" information needed to do your job effectively.
- If applicable, lock cabinets or drawers containing PHI when not in use.
- Do not use the patient's name in the subject field of an e-mail.
- Double check e-mail addresses before hitting the send button.
- Never use your trash bin to discard documents containing patient information – always use Shred - it containers or shredders.
- Minimize the information listed on patient sign-in sheets to last names only if possible and change the sign in sheet twice a day.
- Be sure patient charts are protected from public view.

II. PATIENT RIGHTS UNDER HIPAA

What rights do patients have under HIPAA?

HIPAA affords patients certain rights with respect to their health information. Under HIPAA patients have the right to:

- Receive a notice regarding our privacy practices (NOPP)
- Request restrictions and confidential communication
- Request access to their health information
- Request corrections to their health information
- Request an accounting of people to whom their information was disclosed

NOTICE of PRIVACY PRACTICES (NOPP)

For detailed information, see HIPAA Policy and Procedure 5001

What is a Notice of Privacy Practices?

The Notice of Privacy Practices (NOPP) describes how Yale will protect patient information, when we can use or share this information without the patient's written authorization, and describes the patient's rights with respect to their health information. A copy of the Yale NOPP is available at http://hipaa.yale.edu/

How do we provide notice to patients?

HIPAA requires that we provide all patients with a copy of our Notice of Privacy Practices (NOPP) and that the NOPP be posted in clinical areas as well as on our web site. The NOPP was significantly revised in 2013 and is available at hipaa.yale.edu New patients and those who request it must be given a copy of our NOPP. Returning patients may be provided with a summary of the changes.

Must all patients sign the NOPP acknowledgement?

We are required to provide a copy of the NOPP and to request that patients sign a form indicating that they have received the NOPP. They are not actually required to sign.

Must every clinical area that treats a given patient provide them with the NOPP?

During the course of treatment, a patient may have several appointments throughout Yale's clinical areas. There are some variations in practices between HIPAA covered components

(YSM, YSN, Yale Health, Psychology clinics, and Benefits Office) such that each component is required to provide their own NOPP. However, within each of these components, the practices are the same and thus only one NOPP for that component is required.

For example, a patient seen in Orthopedics at YSM does not also have to get another YSM NOPP if they are also being seen in Diagnostic Radiology. This same patient, however, would need to receive a NOPP from Yale Health if they were seen there as well. Similarly, our close affiliation between YSM and YNHH allows us to use a single NOPP for visits to YSM and YNHH.

How do we know if a patient was already given a NOPP?

When a patient is given the NOPP they are asked to sign the "Acknowledgement of Receipt of the NOPP" form. If the patient doesn't wish to sign, the reason for not signing can be noted on the form as well. Depending on the clinical area, the form itself may be stored in the medical record or the information may be entered into Epic.

REQUESTS for RESTRICTIONS or CONFIDENTIAL COMMUNICATION

For detailed information, see HIPAA Policy and Procedure 5004

What kind of restrictions can a patient put on their health information?

HIPAA allows a patient to ask that we limit how we use and disclose their information in the course of treatment, payment or our healthcare operations. A patient may also request that we not provide information to family members or friends that are involved in caring for that patient. For example, a patient may ask that we not share their information with a particular physician.

Won't restriction requests make it difficult to care for the patient?

Many requests would make it difficult for us to provide quality care and to receive payment for that care. Other requests, such as a request to not share information with those family members who will be caring for the patient may put the patient's health at risk. For these reasons, HIPAA does not require that we accept all requests to restrict uses and disclosures of health information. In fact, in most cases we can not in good conscience accept these requests.

When must we accept a patient's restriction request?

We are required to accept requests by a patient who has paid in full for their treatment and asks that we not disclose information regarding that paid treatment to the patient's health insurer.

What should I do if I get a restriction request?

Since our ability to abide by the requested restriction is determined on a case by case basis, requests for restrictions should be reviewed in collaboration with the Privacy Office.

What is a request for confidential communication?

Confidential communication requests relate to how we contact a patient. For example, a patient may ask that we send information to a P.O. Box rather than a street address or the patient may want to specify a different phone number.

Do we accept these requests?

Yes. Reasonable requests that do not hinder our ability to provide health care should be accommodated.

REQUESTS for ACCESS to HEALTH INFORMATION

For detailed information, see HIPAA Policy and Procedure 5002

How does a patient request access to their health information?

A patient may make a request in writing or via our "Request Access to PHI Retained in the Designated Record Set" form or via signing up for MyChart in those areas where MyChart is available (see https://mychart.ynhhs.org/MyChart-PRD). Patients may ask for either a copy (paper or electronic if available) of their records or for the opportunity to view their records. With 30 days of receiving the request, we are required to provide access to the records or to explain why we can not provide access.

What is the "designated record set"?

For clinical areas, the designated record set includes all medical and billing records related to the individual that we maintain and which we use as the basis for making treatment decisions. For health plans, the designated record set includes all enrollment, payment, claims adjudication, and case record systems maintained by the health plan. For a more detailed list of what should be included in the designated record set see Exhibit 5002 of HIPAA Policy 5002 at www.hipaa.yale.edu

Are there any limits to what information we provide to the patient?

Yes. We are only required to provide the information maintained in the designated record set. Other information we have related to a patient may not be included in the designated record set and we would not be required to provide this information. For example research data which is not related to treatment can be excluded from the designated record set.

Can we ever deny access?

There are a few limited circumstances in which we can deny access to a patient's records or a portion of their records. Decisions to deny access must be made in consultation with the Privacy Office.

Who can request access to a child's information?

In Connecticut children are generally those under 18 years of age and requests may be made by a parent to obtain access to the child's records. State law limits parental access to some information for adolescents, such as mental health and reproductive health records. For more detailed information regarding who can act on behalf of a child, see HIPAA policy and procedure 5038 "Personal Representatives."

Are there other people who can request access on behalf of a patient?

The patient's personal representative may act on their behalf regarding access to the patient's health information. Personal representatives are defined under state law such as an individual's guardian or conservator. See HIPAA policy and procedure 5038 "Personal Representatives."

As an employee how do I access my information?

Employees who are also patients and who have access to the electronic health record due to their position at Yale may access their own electronic record for the sole purposes of reviewing and/or printing their health information. Employee access and safeguarding of information must be conducted in accordance with all applicable HIPAA Privacy and Security policies. Access to Protected Health Information of a family member, including a family member who the employee is an authorized representative of (minor children, etc) must be obtained by following standard patient access processes and may not be obtained by direct access to the electronic record by the requesting employee.

REQUESTS for CORRECTIONS to HEALTH INFORMATION

For detailed information, see HIPAA Policy and Procedure 5002

If a patient finds a mistake in their record, can we just change it?

Patients can request a change to their record using the "Request Amendment of PHI Retained in Designated Record Set" form. If the requested change is valid, then the change can be made. Good medical records practice however requires that the change be appropriately documented. In the case of medical records, the incorrect information can be crossed out and the correct information added. The individual making the change should note their name in the record as the individual correcting the record. If the form is used, the form should be filed/uploaded with the record.

What if the correction requested isn't right?

We can deny a requested change to the record in defined circumstances such as when we did not create the record or we believe that the information is accurate and complete. Denial of an amendment request requires that we notify the patient in writing of the reason for denial. A decision to deny an amendment should be made in consultation with the Privacy Office.

ACCOUNTING of DISCLOSURES

For detailed information, see HIPAA Policy and Procedure 5003

What information are we required to account for?

We are required to keep a listing of individuals outside of the Yale covered components (YSM, YSN, YUHS, YUHP, Psychology clinics, and Benefits Office) to whom we have provided PHI if that disclosure was not for treatment, payment, healthcare operations or as authorized by the patient.

Some examples of disclosures subject to accounting include:

- Public health activities such as communicable disease reporting
- Health oversight activities and audits
- Workers compensation disclosures if not accompanied by an authorization
- Misdirected mailings and faxes and other errors
- Lost records

What information must we include in the listing?

We need to keep a list of what information was disclosed, when, to whom and why we disclosed the information. An excel form is available at www.hipaa.yale.edu for recording this information.

How do we keep this information?

Each clinical area has slightly different procedures for maintaining the accounting logs. At YSM, the log is maintained by the Deputy HIPAA Privacy Officer and spreadsheets should be submitted to hipaa@yale.edu. In other areas, the log is maintained in the medical record. Check with your supervisor regarding appropriate processes in your area.

How do we respond to a patient's request for an accounting of disclosures?

Patients should provide their request in writing, preferably via the "Request for Accounting of Disclosures" form and a copy of the completed form should be forwarded to the appropriate Deputy HIPAA Privacy Officer or to the Privacy Office who will assist in generating the appropriate list. We are required to respond within 60 days of the request.

III. ADMINISTRATIVE ASPECTS of HIPAA
BA's, Fundraising and Marketing

BUSINESS ASSOCIATES

What is a Business Associate?

A Business Associate is an individual or company who is not employed by Yale but who performs or assists us in performing activities that require receiving, creating, storing, transmitting, accessing, using or disclosing PHI (protected health information).

What are some examples of the functions and /or services that Business Associates may provide?

Some examples of the functions and/or services provided by a Business Associate are:

- Claims processing, data analysis or case management services
- Benefit management
- Accreditation
- Paper recycling and shredder companies
- Transcription and record copy services
- Offsite storage
- Repair, upgrade or maintenance of PCs, computer equipment, or software where access to PHI is necessary to provide the service
- External auditors
- Third party administrators of benefit plans

Is everyone who provides a function or service considered a Business Associate?

Providers of certain services where access to PHI is incidental or are not related to our role as a health care provider/health plan are not considered business associates. Examples include:

- Janitorial services and waste disposal of sealed materials
- Repair, upgrade or maintenance of PCs where access to PHI **is not** necessary to provide the service
- Research collaborators and research related services
- State mandated registries such as the tumor registry

How do I determine if the provider of the function or service is a Business Associate?

Department staff should determine if PHI is received, transmitted, stored, created, accessed, used, disclosed or exchanged between Yale and the outside provider. If so, the next question is whether or not the service is performed on our behalf in our role as a health care provider or

health plan. If it is determined that a business associate agreement is needed, a completed Business Associate Tracking form, available at http://www.yale.edu/procurement/hipaaCompliance/index.html should be sent to the HIPAA Privacy Office to initiate the process. If you are unsure, you can consult with the HIPAA Privacy office in making the determination.

More detailed information is available in Yale HIPAA policy 5033 at http://hipaa.yale.edu/policies-procedures-forms

Are all Business Associates required to sign agreements?

The covered components of Yale are required to comply with the Business Associate standard of HIPAA. This standard mandates that Business Associates who may receive, use, obtain, create, store, transmit, or have access to PHI be required to sign an agreement ensuring that the Business Associate will safeguard and protect the integrity, availability and confidentiality of the PHI.

Business associate language incorporated into signed contracts will fulfill the requirement of a signed Business Associate Agreement.

For additional information and forms go to: http://hipaa.yale.edu/policies-procedures/tracking-management-business-associates

If BA language is included in a contract is there more that I need to do?

BAs must be tracked by the HIPAA Privacy Office. If the HIPAA Privacy Office has not been involved in reviewing the BA terms, a tracking form should be sent to the HIPAA Privacy Office to ensure that the arrangement is appropriately monitored.

MARKETING

What is marketing under the HIPAA Privacy Rule?

The HIPAA privacy rule defines marketing as a communication, in any form, about a product or service that encourages recipients to purchase or use the product or service. The definition also includes when a third party pays a covered entity, such as Yale University, to disclose PHI that enables the third party to use the information for its own marketing purposes.

For example, providing a list of diabetic patients to a company that sells glucose monitoring kits would be considered marketing.

What restrictions does HIPAA place on marketing activities?

If the activity qualifies as marketing under the HIPAA definition and is not one of the exceptions, a signed patient authorization is required. The authorization must be specific to the marketing activity and list any payment involved.

For detailed information see HIPAA Policy 5034 at http://hipaa.yale.edu/policies-procedures-forms

Are there exceptions to the communication definition of marketing?

HIPAA does carve out a few exceptions to the definition of marketing. Yale can communicate to patients about various goods and services essential for quality health care when it:

- ☐ relates to Yale's own products or services, such as sending information to our patients about a new service we are providing.
- ☐ is made for treatment of the individual, such as recommending over the counter remedies.
- ☐ is made for case management or care coordination for the individual, including directing or recommending alternative treatments, therapies, health care providers, or settings of care to the individual.
- ☐ is in the form of a face to face communication made by a clinician to the patient.
- ☐ is a promotional gift of nominal value.

Can a business associate handle the marketing for the Yale?

If the communication is permissible under the HIPAA privacy rule Yale may use a business associate to relate some of the communication. As with any disclosure of PHI to a business associate, a business associate agreement must be signed, protecting the use of PHI for communication activities.

For additional information see: HIPAA Policy 5034 at http://hipaa.yale.edu/policies-procedures-forms

FUNDRAISING

Can patient protected health information (PHI) be used for fundraising purposes?

Yes. Yale's Notice of Privacy Practices states that patient demographic, health status data and dates of service information may be used for fundraising purposes without first obtaining

patient authorization. As of March 26, 2013, these types of PHI were expanded to include the following:

- Patient Name
- Address and other contact information
- Gender and age (including date of birth)
- Dates of health care services provided to the patient
- Department of service
- Treating physician
- Outcome information
- Health insurance status

If **any other types of patient information** are to be used in fund raising, we **must** first obtain a specific Authorization from the patient. Diagnosis information or subspecialty information may not be used. Our HIPAA authorization form can be found at http://hipaa.yale.edu/forms/ysm/Form5031YSMHIP11.pdf

Can development officers review lists of patients with physicians to determine the appropriateness of sending fundraising materials or to design a strategy to engage patients in potential gift conversations?

Yes. Physicians can assist the development office by considering whether a given patient is appropriate to contact given their treatment outcomes.

Who can access this patient PHI information for fundraising purposes?

Fundraising information can be used by the Yale School of Medicine development office staff; all staff members are trained in HIPAA Privacy and Security Rule requirements and comply with the University HIPAA policies, including data security requirements. In addition, this patient PHI information may be disclosed to an external entity under contract as a HIPAA Business Associate. Information on whether a company is a Yale HIPAA Business Associate is available at http://hipaa.yale.edu/business-associates/index.html

Is an Opt-Out Provision required in all fundraising materials?

Yes. All Yale School of Medicine solicitations must include, in a clear and conspicuous manner, the opportunity for the recipient to "opt out" of receiving any future fundraising communications. The method of opting out may not require the patient to endure an undue burden such as sending a letter. All Yale School of Medicine solicitations will provide local and toll free phone numbers, a mailing address and an email address so patients will have multiple methods to request to "opt out".

What if a patient opts out of receiving fundraising materials?

When an individual elects not to receive any further fundraising communications that individual will be removed from the fundraising communication list and no future fundraising communications may be sent to the patient. The Yale School of Medicine development office will maintain a list of those patients who request removal from fund raising lists. This information will also be maintained in the patient's medical record.

Can patients opt back in to receive future fundraising materials?

Yes; but receipt of a gift is not an automatic "opt back in". In these cases, development officers will contact the patient donors and determine their willingness to "opt back in". When a patient changes his or her mind and requests to begin receiving fundraising communications, that patient will be asked to sign an Authorization. Once the Authorization is received, they will be added to the list of patients who receive fundraising solicitations.

Are there other requirements for the Development Office related to their use of PHI?

Handling PHI on behalf of a HIPAA Covered Entity requires that the Development Office staff be trained in HIPAA Privacy and Security Rule requirements and comply with the University HIPAA policies, including data security requirements.

Where can I get more information?

For more information please contact the HIPAA Privacy Office at 432-5919 or YSM Development at 436-8560

IV. HIPAA and PATIENT CARE

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 at http://hipaa.yale.edu/policies-procedures-forms

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 at: http://hipaa.yale.edu/policies-procedures-forms

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 gun shot 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 at http://hipaa.yale.edu/policies-procedures-forms

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 at http://hipaa.yale.edu/policies-procedures-forms

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 at http://hipaa.yale.edu/policies-procedures-forms

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 at http://hipaa.yale.edu/policies-procedures-forms

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

V. HIPAA and RESEARCH

What is meant by "use" and "disclosure" in reference to PHI?

"Use" – refers to PHI that is used ***within*** an institution or covered entity such as Yale.
"Disclosure"- refers to PHI that is disclosed to others ***outside*** an institution or covered entity.

HIPAA allows the covered entity certain uses and disclosures of PHI, primarily those related to treatment and payment. Other uses or disclosures are limited to a defined list of activities or with a patient's authorization. Patients are notified of these uses at the time of treatment through Yale's Notice of Privacy Practices (NOPP, see HIPAA Policy and Procedure 5001). For example, we can disclose PHI to insurers in the course of billing for clinical services without obtaining a signed authorization for each billing.

Note that disclosures can occur both by sharing information with individuals who are not affiliated with Yale as well as sharing with individuals who are affiliated with Yale but are not within the covered entity. For example, YSM sharing PHI with the Anthropology Department would constitute a disclosure.

What research activities are subject to the HIPAA Privacy Rule?

Research activities that take place within the Yale covered entity and which involve PHI are subject to the HIPAA Privacy Rule. This includes not only studies where data is collected from research subjects on site but also studies where PHI is collected elsewhere and stored and/or analyzed within the Yale covered entity.

What HIPAA privacy requirements relate to research?

HIPAA does not create explicit requirements for research per se. Instead, HIPAA limits how identified health information can be accessed, used, and disclosed. The HIPAA privacy requirements do not replace or eliminate the requirements of the federal Common Rule (e.g. IRB approval of human subject research) but rather add certain new requirements such as:

- The use or disclosure of PHI for research purposes requires a signed Research Authorization Form from the research subject unless an exception under HIPAA applies.
- Unlike the Common Rule, HIPAA also applies to research on decedents or studies determined to be exempt from IRB review.
- HIPAA requires that only the "minimum necessary" PHI be used.

What is meant by the "minimum necessary" standard in research?

HIPAA requires that only the minimum necessary PHI needed to accomplish the research initiative and the intended purpose of the use and/or disclosure of the PHI be accessed. Information which is

not directly related to the research and which is not indicated in the IRB approved protocol should not be accessed or collected.

Do all types of research fall under the HIPAA Privacy Rule?

The types of research that do not fall under the HIPAA Privacy Rule are:

- Research that does not involve health information
- Research using de-identified data, i.e., data that contains none of the 18 HIPAA identifiers.
- Research conducted by an individual who is not part of a HIPAA covered entity and that does not require access to information held by a HIPAA covered entity.

What is the difference between De-identified data and anonymous data?

"De-identified" is a term used in the HIPAA Privacy Rule and is defined as information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. The Privacy Rule then defines 18 identifiers which must be removed from a data set for that data set to be deemed "de-identified." When all 18 identifiers are removed, the data is no longer identifiable and thus no longer PHI which means that HIPAA no longer applies.

"Anonymous" is not defined in either the Privacy Rule or Common Rule but has been used by IRBs to refer to data which does not meet the Common Rule standard of individually identifiable private information. The Common Rule does not define what constitutes an identifier; rather it defines individually identified private information as that for which the identity of the subject is or may readily be ascertained by the investigator or associated with the information.

Because the Privacy Rule is more prescriptive of what constitutes an identifier than the Common Rule, it is possible to have data which would be considered "anonymous" by an IRB but not meet the HIPAA standards for de-identification. In such cases, the Common Rule may not apply or the study qualifies for exemption but HIPAA would still be applicable. For example, a data set which included dates of service for a large sample size is identified under HIPAA but may be deemed anonymous under the Common Rule.

Can de-identified data or anonymous data also be coded?

HIPAA allows disclosure of de-identified data that is coded as long as the code is not derived from identifiers and the code is not disclosed with the data. Researcher A or Hospital A can therefore create a coded de-identified data set for use by Researcher B as long as the code isn't also shared. Researcher B's work with the data is not covered by HIPAA as Researcher B does not have PHI. Researcher A has both the data and the code and hence is subject to the HIPAA requirements.

Similarly, the Common Rule does not pertain to research that does not involve human subjects, e.g. does not involve intervention or interaction or which does not involve identifiable private information. Data can be coded and not be considered to involve human subjects as long as the code is not provided to the researcher and the code itself does not identify the individuals. In the example above, when data is provided to Researcher B with a code and Researcher B agrees in writing to not obtain the code, then the coded data is not covered by the Common Rule. Similarly, if the data owner has policies and procedures which prohibit release of the code, then the data can also be deemed to not involve human subjects and hence not subject to the Common Rule requirements. Determinations regarding whether or not a study involves human subjects as defined under the regulations should be done in consultation with the IRB.

Under the HIPAA Privacy Rule is a research authorization needed?

As a general rule, in order to use PHI in research it is necessary to obtain a signed authorization form from each research subject prior to creating, using or disclosing PHI. The requirement for a HIPAA authorization is in addition to the requirements for informed consent, although in some cases the two can be combined (see below). Yale has developed a Research Authorization Form (RAF) and compound authorization template which include the specific elements mandated by the HIPAA Privacy Rule.

See: HIPAA Policy and Form 5032: http://hipaa.yale.edu/policies-procedures-forms

Does a new RAF need to be submitted each year with the protocol renewal application?

No. Unless there is a change to the project which necessitates a change in the RAF, such as when a new collaborating institution is to be provided access to the PHI, the RAF does not have to be submitted for continuing review by the IRB.

Must the Yale University RAF/Compound Authorization template always be used?

The Yale University Research Authorization Form (RAF) and the Compound Authorization Template provide standard language for the required HIPAA Privacy Rule research authorization. PIs using either of these forms need only specify to whom and where PHI will be sent and what type of PHI will be disclosed. Authorization forms not based on the Yale template or that modify or remove language from the template are subject to review by the Privacy Office and IRB to ensure that they are valid under HIPAA's requirements.

What if the PI needs to disclose PHI to a person or organization not listed in the original signed RAF?

Permissible uses and disclosures are limited to those detailed in the original signed RAF and in the case of studies that also involve treatment, in the Yale Notice of Privacy Practices (NOPP, see HIPAA Policy and Procedure 5001). Note that the NOPP describes permissible disclosures related to our providing health care and does not substitute the need for a RAF in the research context. The NOPP does however allow disclosure for payment in the case of trials which will bill insurers for health care services. If a researcher needs to disclose PHI to a person or organization not listed in the signed RAF for research related purposes, the researcher should obtain an additional written RAF from the subject or apply to the IRB for a waiver of Authorization. Disclosure of PHI without patient authorization requires that the disclosure be logged in the accounting for disclosure log.

When is a RAF waiver needed? (HIPAA Authorization)

If PHI is to be used or disclosed and no written authorization has been or is planned to be obtained from the research subject, a researcher must submit a request for a waiver of authorization to the IRB. The waiver will be approved if **all** of the following conditions exist:

- The research could not practicably be conducted without the waiver
- The research could not be practicably conducted without access to and use of the PHI
- A written assurance is provided to the IRB that the PHI will not be re-used or disclosed except as required by law, for authorized oversight of the research, or for other IRB-approved research
- Uses and disclosures of PHI will be limited to the "minimum necessary" standard
- Disclosure involves no more than minimal privacy risk to the individual.

If a waiver of authorization is not approved, the PHI cannot be used or disclosed as planned in the described research and a signed RAF must be obtained from each research subject.
Disclosures of PHI that are made in connection with research conducted pursuant to a Waiver of HIPAA Authorization must be tracked in the event the subject requests an accounting of disclosures of their PHI.

Is a signed RAF needed when recruiting participants?

The recruitment procedure frequently requires access to a limited amount of health information and therefore the PI must comply with HIPAA requirements of obtaining either a signed RAF from the patient or a Waiver of HIPAA Authorization approved by the IRB prior to using PHI to determining eligibility or recruitment activities. When the RAF is waived for recruitment only, it is referred to as a ***"partial waiver"*** because following recruitment a RAF will need to be signed by the research subjects.

Do I need a waiver if the authorization will be done orally?

Yes. HIPAA does not have provisions for authorization to be provided in any way other than a written form signed by the patient/subject. For example, if the information will be read to the subject over the phone or presented on-line at the start of a survey, a waiver of authorization is required to accommodate the lack of signature.

What is the difference between an informed consent and a RAF?

Simply stated, informed consent refers to the subject agreeing to participate in the research, while a RAF refers to the subject (or research participant) giving permission to use and disclose their PHI (protected health information). The requirements of the RAF under HIPAA are different from the Common Rule consent form requirements; for example, the consent form does not require the specificity of who will have access to the data. On the other hand, the RAF does not need to explain the non-privacy risks of the research. The two do overlap and can often be combined in a compound authorization.

HIPAA Authorizations vs Common Rule Consent

	Common Rule	HIPAA
Statement that study involves research	X	
Purpose of the research/disclosure	X	X
Duration of participation	X	
Description of procedures	X	
Description of risk	X	
Description of benefits	X	
Description of alternate procedures/treatments	X	
Degree of confidentiality	X	
Description of compensation/treatment for injury	X	
Who to contact for research questions	X	
Who to contact for questions about their rights	X	
Who to contact in case of injury	X	
Statement of voluntary participation/no loss of benefits/treatment if don't participate	X	X
Ability to withdraw/revoke and any exceptions	X	X
Potential for unknown risks	X	
Potential to be withdrawn from study by PI	X	
Costs of participating	X	
Consequences of subject withdrawing from study	X	
Promise to provide additional information during the course of the study	X	
Number of subjects	X	
No exculpatory language	X	
Signature	X	X
Date		X

Specific description of information to be used/disclosed	X	X
Who is authorized to use/disclose the information		X
To whom the information can be used/disclosed		X
Expiration date of authorization (not of form)		X
Potential for re-disclosure and no longer protected		X

What is a compound authorization?

A compound authorization combines the required elements of the Common Rule consent form and those required in a HIPAA Research Authorization form (RAF) into a single document.

When can you use a compound authorization?

Since RAFs are sometimes used to authorize release of subject medical records, they can end up filed in a medical record. When a compound authorization is used, both the consent information and RAF information end up in the medical record. Consent forms generally provide more detailed information which may be inappropriate for inclusion in a medical record. In such cases, separate consent and authorization forms should be used. A compound authorization can be utilized when the privacy risks associated with using a document containing both consent and authorization information are minimal.

Can banking of specimens obtained from research be included in a compound authorization?

The HIPAA Privacy Rule considers the creation and maintenance of a research repository or database as a specific research activity which can be authorized via the RAF, which in some cases may be a compound authorization. In cases where the banking of biological specimens is in addition to the current research protocol, subjects should be given the ability to consent to the research but not to the banking. This can be achieved using checkboxes on the compound authorization which allow the subject to specify whether or not they are consenting to both the study and the banking.

When is the "Request for Access to PHI for Research Purposes" form used?

The "Request Access to Protected Health Information for a Research Purpose" document, located with HIPAA Policy 5032, Use and Disclosure of PHI for Research Purposes at: http://hipaa.yale.edu/policies-procedures-forms is meant for use by investigators requesting access to protected health information for research purposes including activities preparatory to research. Once completed, it should be submitted with the supporting documentation (described on the form) and given to the entity responsible for the PHI of interest. Both Yale University and Yale New Haven Hospital (YNHH) have approved this form and it can be uploaded into the documents tab of Epic.

What is a limited data set?

A limited data set is PHI that excludes "direct identifiers" of the individual, relatives of the individual, employers, or household members of the individual and excludes psychotherapy notes. Limited data sets do not meet the strict HIPAA definition of "de-identified" data but present only minimal potential for identifying the participants. Limited data sets are afforded exception from HIPAA's accounting for disclosure requirement and are a useful way to minimize the HIPAA burden on research when used appropriately.
In contrast to de-identified data, limited data sets can have geographic areas and elements of dates, for example: Epidemiology research studies may have data where the subject names are not needed but geographic locations are relevant and a limited data set may be used.

A limited data set can only be used for purposes of research, public health, or health care operations and if the covered entity providing the data and the recipient of the data first enter into a Data Use Agreement.

What is a data use agreement?

A data use agreement is an agreement between a covered entity (the holder of the PHI) and the recipient of the PHI (such as a research investigator) in which the covered entity discloses a limited data set for purposes of research, public health or healthcare operations. Data use agreements outline permissible uses and disclosures of PHI and prohibit re-identifying or using the PHI to contact individuals.

What is an internal data use agreement?

An internal use data use agreement is used for passing limited data sets within Yale or for studies where the HIPAA privacy rules do not apply initially but becomes applicable following data collection. For example, studies conducted at facilities outside of the U.S. or health information collected from an educational record are not governed by HIPAA while the data reside outside the US or in the school. However, once the data are transferred to a HIPAA covered entity, such as YSM, all HIPAA regulations apply. Yale developed the internal data use agreement to allow researchers working internationally to bring limited data sets back to Yale with only a minimal HIPAA burden.

VI. HIPAA and the Benefits Office

Is the Yale University's Benefits Office a covered entity under the HIPAA Privacy Rule?

HIPAA applies to both healthcare providers and to health plans.

One function of the Benefits Office is the administration of the various medical, dental and insurance benefit plans offered through the University. In this role, the Benefits Office is required to comply with HIPAA.

Are any of the functions of the Benefits Office excluded from the HIPAA Privacy Rule?

Yes, the Benefit's Office's role in Workers Compensation cases and Long-term disability cases are excluded from the HIPAA Privacy Rule. However, the information associated with these functions must still be treated with the appropriate respect for the confidentiality and dignity of the individuals affected.

Is everyone in the Benefits Office required to take the HIPAA training?

All employees who work in the Benefits Office, including casuals and temporary staff, are required to complete the HIPAA training module at the start of their employment.

Can an employee of the Benefits Office obtain PHI without a written authorization from a staff member when assisting with a claim for benefits?

When a University employee asks for help in obtaining proper reimbursement for a claim, the Benefits Office staff may use and disclose the employee's PHI to assist in processing the claim.

Can PHI be disclosed to a family member or individual who calls to inquire about a claim?

Claim status information may be disclosed to a family member or individual when the individual provides information that demonstrates that they are involved in handling claim matters for the member, provided that the member has not previously requested any restrictions of such disclosures.

Can a union representative who may be representing me in a benefits dispute obtain PHI from the Benefits Office on my behalf?

Unlike the Benefits Office staff who are involved in administering the University's benefits plans, other employees or union representatives would not have authority to access or obtain PHI on behalf of an employee without a signed HIPAA authorization, even when assisting in a claim resolution. However, if the union representative contacts the Benefits Office together with the member, the Benefits Office staff could disclose the member's PHI to the union representative if the member verbally agrees to the disclosure.

Under the HIPAA Privacy Rule are all members of health plans to be provided with a Notice of Privacy Practice (NOPP)?

Yes, health plans must provide covered members with a copy of the NOPP at the start of their enrollment in the plan. In addition, every three years the health plan is required to notify individuals covered by the plan of the availability of the NOPP and how to obtain the notice. Also, if a revision to the NOPP is made, then the health plan must notify those enrolled within 60 days of the change.

Note that the individual health insurance plans (e.g., Aetna, Yale Health, Delta Dental, etc.) provide the Notice of Privacy Practices on behalf of University. In some cases, the Notice is provided to the subscriber employee on behalf of both the subscriber and their dependents.

Can the subscriber act on behalf of the other dependents listed on the policy?

The employee who is the actual subscriber on the benefit plan may act on behalf of their dependent members such as spouse, partner, or children, listed on the policy for various plan administration purposes such as enrollment, premium payments, health insurance claims and benefit related concerns.

How does the Benefits Office protect PHI that it may receive on behalf of an employee and/or their dependents?

Any PHI that the Benefits Office may receive must be protected under the HIPAA Privacy Rule. In addition to the physical safeguards, the Benefits Office protects any PHI it may receive by maintaining a "firewall" that limits how and which staff members may use, disclose, discuss and/or review the PHI of employees and their dependents. In particular, information is not allowed to be shared with human resources or personnel without authorization by the employee.

Does HIPAA prohibit Yale from using health information for employment related decisions?

In general, HIPAA prohibits an employer from using PHI for employment determination unless the employee has signed an authorization. However, if the employer requested specific test and services as part of pre and continued employment requirements these would not be considered PHI and therefore not protected under the HIPAA Privacy Rule. For example, employee health monitoring by the Office of Environmental Health and Safety is not covered under the HIPAA Privacy Rule.