Frequently Asked Questions

FAQs

- What is HIPAA?
- What is the Privacy Office and what do they do?
- There has been a breach of patient privacy in my department. What do I do?
- How do I know what HIPAA and privacy training should be provided to the people in my department?
- I want to provide a flyer to a specific patient population, produced by an outside organization (i.e., American Heart Association). May I do this?
- How much personal information may be released to family members over the phone?
- What is my responsibility related to the vendors that I bring into the Medical Center?
- My patient does not answer the phone directly. How can I leave a HIPAA compliant message with someone else or a voice mail?
- My patient is now on another unit. May I access their record?
- May I email my patient related to his or her care?
- How much information may I give an Insurance company?
- How much information may I give a Skilled Nursing Facility (SNF) or Home Health Agency (HHA)?
- How much information may I give to a police officer?
- What information may be faxed?
- May I mail my patient's information?
- My patient's insurance company is requesting information in relations to a Worker's Compensation claim. What information may I provide?
- Someone wants to come into a clinical area and observe. How can I make this happen?
- We use a sign in sheet for our patients. Is that ok?
- What information may be listed on dry erase whiteboards?
- I purchased a new laptop. May I use it for work purposes? And if so, how do I protect it?
- I have access to clinical systems and my husband asked that I look up his record to check that his physician's notes were correctly entered. Based on his explicit request, am I allowed to access his medical records?
- How does an adolescent (12-17 years) authorize granting proxy access to a Parent/Guardian?
- When is it OK to share PHI?

For additional FAQs, related to HIPAA please refer to the U.S. Department of Health & Human Services HIPAA Frequently Asked Questions [1].

What is HIPAA?

The Health Insurance Portability and Accountability Act (HIPAA) was passed to protect the confidential medical and billing records of our patients. A particularly important element of HIPAA regulation pertains to patients’ rights related to access and control of their medical information. We count on all members of the UCSF entity to incorporate the HIPAA rules into
their daily activities. Our patients have a right to privacy. We are committed to complying with HIPAA, not only because it is the law, but also because we value our patients and their privacy. For details refer to the UCSF Privacy and Confidentiality Handbook [2].

What is the Privacy Office and what do they do?

The Privacy Office is responsible for monitoring compliance with the federal and state privacy laws and regulations. The Privacy Office is responsible for orchestrating departmental responses in the event of a breach of patient privacy. Additionally, the Privacy Office provides consultation on requests for all privacy related questions. The Privacy Office tracks and analyzes all privacy activities, and develops training and risk mitigation programs for the entire UCSF enterprise.

There has been a breach of patient privacy in my department. What do I do?

If the personally identifiable information was on a stolen device (computer or PDA, for example), immediately contact UCSF Campus Police [3] (415-476-1414) to report the theft, and if personal health information is involved, contact the Privacy Office (415-353-2750). The UCSF Campus Police will contact ITS. For disclosures not involving a stolen device, contact the Privacy Office immediately.

In every circumstance, you will need to provide the following information:

- Date and time the breach was discovered
- Name and contact information of the person who discovered the breach
- The specific information disclosed
- The number of individuals who had their information disclosed
- How the breach happened
- Actions taken following detection
- The department contact for follow-up

The department is responsible, under the direction of the Privacy Office, for the follow-up including, but not limited to, the investigation, patient notification and follow-up, determining and implementing corrective actions and changes in process, following-up with third party vendors, retraining personnel, and documentation, as needed. Please note that only the Privacy Office can determine if notification is required.

Privacy breaches need to be reported to the Privacy Office as soon as they are discovered, even if the person who discovered the breach was not involved. Any delay in reporting to the UCSF privacy office delays UCSF reporting to the state and to patients. Delayed reporting to the state and patients beyond the 5 day timeframe exposes you and the University to financial liability in the way of administrative fines and penalties.

You will not be penalized for reporting breaches, nor does the reporting of a breach necessarily implicate you in any way.
How do I know what HIPAA and privacy training should be provided to the people in my department?

Refer to the Education and Training section of the Privacy Office website. Remember, all members of a department need to have some type of training, including volunteers, and all training must be documented. The Department is responsible for ensuring its staff members are properly trained, and for maintaining documentation of such. Training includes:

I want to provide a flyer to a specific patient population, produced by an outside organization (i.e., American Heart Association). May I do this?

You can post the flyer in the clinic waiting room for interested patients. Additionally, any mass mailings that go out to patients for fundraising purposes must follow the established UCSF process and be approved by UDAR as there are certain restrictions and required inclusions. See the Fundraising section for details. Any use of the UCSF logo associated with another organization needs to be approved by University Relations (415-476-8252).

How much personal information may be released to family members over the phone?

According to the Notice of Privacy Practices, you may release personal information to anyone that the patient has identified as the recipient of such information. Refer all others to the contact person the patient designates. In all other cases, or if no contact person exists, you are not authorized to release any information other than whether or not the patient is in the hospital and his or her general condition (e.g., good, fair, critical). If the patient is hospitalized, certain limited information can be found in the hospital directory so that family, friends, and clergy can locate the patient. Good practice involves requiring the requestor to provide the patient’s full name, verifying their identity and relationship to the patient, and only supplying the minimum amount of information necessary.

What is my responsibility related to the vendors that I bring into the Medical Center?

Before allowing vendors access to the Medical Center, they must check in with Material Services. Once this is complete, they should be wearing a Visitor ID at all times while in the Medical Center. Do not leave vendors alone in areas with PHI that they do not need to have access to (i.e., clinic work areas). It is recommended that they wait in the waiting room or in a designated conference room.

My patient does not answer the phone directly. How can I leave a HIPAA
compliant message with someone else or a voice mail?

Leave the minimum amount of information needed: your name, phone number and that you are from UCSF. A recommended best practice would be to obtain the patients preference for follow up or appointment communication at the initial point of contact.

back to top

My patient is now on another unit. May I access their record?

You may access the patient?s record only if you have a legitimate need to do so (for treatment, payment, or health care operations). Otherwise, you should not access the record.

back to top

May I email my patient related to his or her care?

As long as the patient has not requested otherwise, you may do so but only by following the secure email guidelines on the IT Security page. Best practice includes making sure the patient prefers this form of communication and understands the risks associated with it.

back to top

How much information may I give an Insurance company?

According to Notice of Privacy Practice, we may use and disclose medical information for the purpose of obtaining payment. Best practice is to only provide what is needed for this purpose. For example, lab values are not required for billing purposes, and therefore should not be provided to the insurance company. However, if the patient has submitted an Authorization allowing the use and disclosure of his or her information to the insurance company, the minimum necessary standard would no longer apply.

back to top

How much information may I give a Skilled Nursing Facility (SNF) or Home Health Agency (HHA)?

If the patient is being referred to either of these types of facilities, then you have a patient care need to disclose PHI. You should provide all PHI that you feel they need to know to provide continuity of safe patient care.

back to top

How much information may I give to a police officer?

You may disclose protected health information for law enforcement purposes, although you must first verify the identity and authority of the officer requesting the information. In addition, you should limit the PHI released to only the minimum required.

back to top
What information may be faxed?

Always send the minimum information necessary. Best practice is to confirm correct fax number prior to sending, include a cover letter with a confidentiality statement and to ensure receipt via phone call.

back to top

May I mail my patient's information?

Yes, as long as the patient has not requested otherwise, and you have a patient care need to do so. Best practice is to mail only the minimum required, to confirm the correct address with the patient prior to sending, to seal the envelope or package well, and to make sure it does not have any identifying information on the outside besides UCSF.

back to top

My patient's insurance company is requesting information in relations to a Worker’s Compensation claim. What information may I provide?

You are authorized to disclose PHI in order to comply with Worker’s Compensation law. In fact, HIPAA generally allows for the disclosure of patient information to comply with any judicial or administrative proceeding in response to a court order, subpoena, or other legal process.

back to top

Someone wants to come into a clinical area and observe. How can I make this happen?

Guidelines have been developed by HR, Risk, and Privacy to ensure the consistent and appropriate handling of visitors and observers. Various forms, screenings, badges, and/or orientations may be required based on the number of days of observation, the type of observation, and/or whether the observer will interact with patients. Use the matrix at http://hr/forms/compliance.pdf [8] to determine what the compliance requirements are in your particular case. Links to additional forms and information can be found at Visitors and Observers [9] page. Questions and requests for guidance should be directed to Privacy, Risk, Occupational Health, and/or Human Resources.

back to top

We use a sign-in sheet for our patients. Is that okay?

It is OK, however reasonable safeguards and the minimum necessary standard must be met. For example, if using a patient sign-in sheet, do not request any medical information not required for sign-in. Also, consider a pull-off label system or a thick black marker to cross off names as patients are called in for their appointments, such that patient names do not accumulate throughout the day for subsequent patients to view.
What information may be listed on a dry erase whiteboards?

The use of whiteboards is allowed as long as reasonable safeguards are implemented, as appropriate. Listing only last name and first initial in the department is adequate, whereas full first and last name are permitted for safety reasons in the operating room. The important considerations are whether the board is visible to passers-by and whether it contains PHI. If yes to both, consider whether there are other ways that the protected data (including demographic data) could be "reasonably" limited to the minimum necessary to allow the unit to safely manage patient care.

I purchased a new laptop. May I use it for work purposes? And if so, how do I protect it?

You should avoid using any personal devices for work purposes. If you must use your personal laptop for work purposes, discuss it with your Manager first. If your manager approves, ensure that your computer is encrypted and that it meets all the other requirements of the UCSF Minimum Security Standards (http://tiny.ucsf.edu/mss [10]). Guidance on encrypting your laptop can be found here [11]. Guidance on the software you should install is at http://software.ucsf.edu [12]. The best practice is to consult with IT before use to ensure proper security through firewalls, passwords, anti-virus software, regular software updates, and more (contact IT at 415-541-4100). Always follow best practices, including maintaining physical security of your device at all times, regular encrypted backups of data, storage of only the very minimum necessary patient information, and the permanent deletion of all data and files the moment they are no longer needed. Remember, it is your responsibility to encrypt and safeguard your device, and you may be held personally liable for breaches of patient information due to an unencrypted, personal device that does not comply with University policy.

I have access to clinical systems and my husband asked that I look up his record to check that his physician’s notes were correctly entered. Based on his explicit request, am I allowed to access his medical records?

No. You are not authorized to directly access the medical records of any individual whose care you are not involved with. Your husband should contact HIMS to exercise his right to request an inspection or copies of his own medical record.

How does an adolescent (12-17 years) authorize granting proxy access to a Parent/Guardian?

MyChart Proxy Authorization form must be completed prior to MyChart signup. This proxy access is automatically removed once the adolescent patient reaches the age of 18, and can be revoked at any time. This proxy access does not include access to sensitive services.
information such as reproductive health and certain mental health and substance use screening and treatments. As certain sections may contain sensitive information, parent/guardian proxy access has limitations which are fully detailed in the MyChart Proxy Authorization form.

When is it OK to share PHI?

While it's prudent to be cautious about sharing and releasing PHI, it's also important to remember that HIPAA allows for the exchange of PHI for purposes of treatment, payment, and operations ("TPO"). The HIPAA Privacy Rule is intended to protect patients' health information, but not to impede or interfere with patient care or safety. Thus, the Rule permits PHI uses and disclosures as needed to provide quick, effective, and high quality healthcare; to bill and receive payment for healthcare services; and to conduct healthcare operations.

The Rule also permits incidental uses and disclosures, and those necessary for national security, disaster notification, law enforcement, public health activities, abuse and neglect reporting, health oversight, organ and tissue donation, health or safety threat aversion, Worker's Compensation, and more. In all cases, the Covered Entity is obligated to apply reasonable safeguards and to implement the Minimum Necessary Standard. In some cases, the release must be documented in an Accounting of Disclosure.

Treatment is the "provision, coordination, or management of health care and related services among health care providers or by a health care provider with a third party." This includes:

- Sharing PHI with the ambulance while the patient is in transport to UCSF
- Consulting with the patient’s other healthcare providers
- Providing PHI when referring or transferring a patient to a laboratory, nursing home, or outside provider or hospital
- Sharing patient information with other UCSF workforce members involved in the patient's care
- Discussing the patient’s condition or treatment regimen in the patient's semi-private room
- Providing therapy to patients in group settings

Payment encompasses all activities to obtain payment or be reimbursed for services provided or the provision of health care. This includes:

- Determining eligibility, reviewing services, and adjudicating claims
- All billing and collection activities, including those of another provider or Covered Entity for its treatment of the patient
- Utilization review
- Speaking with the patient’s guardian or representative regarding bill payment
Operations are "certain administrative, financial, legal, and quality improvement activities of a covered entity that are necessary to run its business and to support the core functions of treatment and payment." This includes:

- Case management, care coordination
- Quality assessments
- Accreditation, certification, licensing, and credentialing
- Legal, audit, privacy, compliance
- Business planning and development
- Administrative activities, including customer service, employee relations activities, transfer of assets, fundraising
- Education and training programs
- Abuse and neglect investigations

If you’re unsure about whether a scenario is considered TPO, simply contact your Manager or the Privacy Office for guidance.

Source URL: https://hipaa.ucsf.edu/frequently-asked-questions

Links