

HIPAA Frequently Asked Questions

Q: Is PHI the same as the medical record?

A: No. HIPAA protects more than the official medical record. A great deal of other information is also considered PHI, such as billing and demographic data. Even the information that a person is a patient here is Protected Health Information.

Q: What if I'm accidentally overheard discussing a patient's PHI record?

A: It is not a violation as long as you were taking reasonable precautions and were discussing the protected health information for a legitimate purpose. The HIPAA privacy rule is not meant to prevent care providers from communicating with each other and their patients during the course of treatment. These "incidental disclosures" are allowed under HIPAA.

Q: If I overhear patient care information in the elevator or in the hallway, how should I handle it?

A: If it seems appropriate, remind the speakers of the policy in private. If the conversation clearly violates policies or regulations, report it to the Privacy Officer.

Q: I work in the hospital and don't need to access PHI for my job, but every now and then a patient's family member asks me about a patient. What should I do?

A: Explain that you do not have access to that information, and refer the individual to the patient's health care provider.

Q: I know that patients have a right to their PHI. What about parents and guardians of incompetent patients?

A: If someone other than the patient has the legal right to make health care decisions for the patient, that person is the patient's personal representative and has the right to access the patient's PHI.

However, if you have good reason to believe that informing the personal representative could result in harm to the patient or others, then you do not have to disclose the PHI.

Q: What should I do if a government agency or law enforcement person requests information about a patient?

A: If working with law enforcement is not part of your responsibility, contact your supervisor. If it is your responsibility, provide only the minimum amount necessary to support the investigation after verification of the authority of the individual or organization making the request.

Please see the Verification section for more information, and always consult your supervisor or the Privacy Officer if you're not sure what to do.

HIPAA Frequently Asked Questions

Q: When the law requires me to make a disclosure, such as reporting HIV infection, do I need to tell the patient that I disclosed the information?

A: You need to tell the patient only if they ask for an accounting of disclosures, and the disclosure was made without an authorization.

If there is good reason to believe that informing the patient could result in harm to that individual, then you may not be required to tell him or her. In some cases, government agencies can also require that the patient not be informed. If you are in doubt, contact the Privacy Officer for advice.

Q: Do I need to record the fact that I've made these disclosures?

A: For the most part, yes. You need to document most disclosures made without authorizations except disclosures made for TPO purposes. Your unit should have procedures for documenting them.

Q: As part of my job, I have access to a patient's PHI. How do I know which family and friends can be told this information?

A: Always ask the patient who can receive this information and document the patient's response in the medical record.

Q: When I am speaking to a patient, and friends or family members are in the treatment room, do I assume the patient has given me permission to speak of the PHI in front of these persons or do I need to ask them to leave?

A: It is proper to speak, unless the patient objects. If you are uncertain, you can ask the patient if it okay to discuss their PHI in front of the person.

Q: If the patient is not conscious, to whom can we disclose the PHI?

A: You will have to decide this on a case-by-case basis. If you know the patient's preferences, as in "you can tell my spouse, but not my sister," then document the request and follow it. Otherwise, use your professional judgment. Always use the Minimum Necessary standard: disclose only information that is directly relevant to the person's involvement with the patient's health care.

Once a patient has regained consciousness, he or she will determine when and how we can share protected information.

Q: Can someone else still pick up a patient's prescriptions, x-rays, or medical supplies?

HIPAA Frequently Asked Questions

A: Yes, if in the care provider's professional judgment it is okay to give the prescription, x-rays or medical supplies to that individual.

Q: If a patient asks for his or her PHI, do I need any special identification from the patient?

A: If the patient is asking for his or her own information, you only need to verify his or her identity.

Q: What if someone from a government agency comes up and asks me for information?

A: It's important to verify that the request is legitimate. Ask to see a picture ID, badge or other official identification before disclosing PHI.

Q: What if I get approached by an individual who just says he's a friend of a patient?

A: Check to see if this individual has been approved by the patient for disclosure of PHI. If so, ask for one or more pieces of identification, including a picture ID.

Q: What if I get a phone call looking for information, and the caller says it's the patient? What should I do?

A: If the request is made by phone, and the requester identifies him- or herself as the patient, you can ask him or her to provide personal information for verification, such as his or her birth date, or Social Security number.

Q: What about requests to leave information on voice mail or an answering machine?

A: If you are asked to phone or leave confidential information via voice mail, for example, you should verify with the patient or other approved individual that it is okay to leave messages this way. Make sure you confirm the number. Your unit may have more restrictive policies, so check with your supervisor or department head.

Q: What if I'm not supposed to leave a message?

A: If you are asked not to leave voice messages, do not do so. This is especially important with patients who may not want to share PHI with family members, roommates, or co-workers.

Q: How much information is it OK to leave?

A: Always leave the minimum possible amount of information.

Q: What if a patient requests that I communicate with him or her via e-mail?

HIPAA Frequently Asked Questions

A: If your unit has specific policies regarding e-mail requests, follow them. Otherwise, here are some things you can do...

1. Inform the patient to not use email for time sensitive matters, as you may be out of the office or busy taking care of other patients.
2. Make sure that patients understand that e-mail is not secure.
3. Do not initiate e-mail with patients without first getting their permission, and only use the e-mail address they provided, unless they notify you of a change.
4. If you receive any request via e-mail, don't assume the sender is the person he or she claims to be, especially if the request is unexpected. If you have not previously verified an e-mail address with the patient, contact either the patient to verify the sender's identity and e-mail address, or contact the person making the request by another method for verification of the e-mail address. If in doubt, talk to your supervisor. In general, be careful about sending PHI in response to e-mails because of the difficulty in identifying senders accurately.
5. Minimize the amount of information disclosed in an e-mail.

Q: I'm a clinician. Are there special rules for me?

A: There will be a standard disclaimer for clinicians to use in their e-mail to patients. It is currently being developed.

Q: What if patients disclose their PHI in an e-mail?

A: If patients disclose their own PHI in an e-mail to you, you can discuss it. However, you should try to avoid disclosing additional PHI in return.

Q: What do I do if I receive a request for PHI by fax?

A: Most often, faxed requests for PHI will come from other health care providers or payers, like billing agencies or insurance companies, although patients may occasionally ask to have information faxed to them.

If a patient, health provider, or payer requests that you fax PHI, get a specific fax number from them and double-check the number before sending.

Q: Is there any way I can make the process more secure?

A: It's a good idea to program commonly used fax numbers to diminish potential dialing errors. If possible, ask the person to whom you've sent a fax to confirm it was received.

Q: What if someone from a government agency sends me a fax asking me for information?

A: Ask for the request to be on official agency letterhead, and call back the indicated number to verify the request is legitimate.

HIPAA Frequently Asked Questions

Q: What if I find a fax went to a wrong number?

A: In the event you find that a fax went to a wrong number, try to retrieve the communications containing the PHI that were faxed to the wrong number, or ensure that they have been destroyed in a secure fashion.

Q: What if I receive a request for PHI on my pager?

A: When communicating via alpha pagers, you should send only the minimum amount of information necessary, and delete received messages once you no longer need them.

Q: I have temporary staff people who will only be here a short time. They need computer access to do their work. Can I give them my password or log them in as me?

A: No. It is against policy to allow any staff, including temporary staff, to use another Health System employee's computer access. If you allow someone to use your access, you will be held responsible for what they do. Your department's authorized signer can make the request for new accounts.

Q: What are the access policies for students?

A: Students working within the Health System must follow the same regulations and policies as regular employees.

Q: What's the safest way to dispose of PHI in the office?

A: Paper records containing PHI should be disposed of in designated confidential recycling receptacles and not in the regular trash.

Q: What will happen if the PHI regulations have been violated?

A: UofM may face civil or criminal penalties and be substantially fined. Further, employees who knowingly misuse protected health information may be subject to prosecution, fines and/or imprisonment up to ten years, in addition to any University disciplinary actions.

The penalties for those who deliberately misuse protected health information are:

For knowing misuse of PHI – up to 1 year imprisonment, or \$50,000 fine, or both

•For obtaining PHI under false pretenses – up to 5 years imprisonment, or \$100,000 fine, or both

•For using PHI for commercial advantage, personal gain, or malicious harm – up to 10 years imprisonment, or \$250,000 fine, or both.