HIPAA Tip Sheet

Jefferson Health HIPAA & Privacy Guide

Important tips on the appropriate access, use and/or disclosure of patients' PHI and other private and confidential patient information

Jefferson is required by law to provide all members of our workforce, including our students, training on the policies and procedures regarding the protection and safeguard of Protected Health Information ("PHI") as necessary and appropriate to carry out their function here at our organization.

It is every member of the Jefferson community's responsibility to safeguard and protect the privacy and security of PHI. It is inappropriate for anyone to access, use or disclose patient information outside of the scope of your job function or student hotspotting responsibilities.

What is Protected Health Information?
PHI is health information about a patient created or received by health care providers and health plans. PHI information includes:

Sent or stored in any form (written, verbal, electronic):
- That identifies the patient or can be used to identify the patient
- That is about a patient's past, present, and/or future treatment and payment of services

PHI is any health information that can lead to the identity of the individual or a reasonable assumption as to the individual's identity

Accessing Health Information
Limit the access, use or disclosure of PHI to the minimum necessary to accomplish the intended purpose. The minimum necessary standard not only addresses whether PHI is shared, but also how much PHI is shared. When accessing patient information, ask yourself the following questions:

Is it necessary in order to perform my job duties?

What is the minimum amount of PHI I need?

Am I following Jefferson's policies and procedures on the confidentiality and security of patient related information?

Jefferson prohibits its Jefferson community members' access to PHI for any reason other than to carry out job-related/student hotspotting duties or to satisfy an approved request.

Use only the minimum amount necessary to perform your job or satisfy the authorized request.
Follow Jefferson's policies and procedures on the confidentiality and security of the patient related information.
DO NOT access, use or disclose PHI or other confidential information for personal gain!
Always maintain a professional demeanor while communicating with patients.
DO NOT engage in inappropriate communication with the patients by any means, including but not limited to:
Emails - Text Messages- Phone Calls - Letters - Social Media Communication - In-Person

Patient Recruitment

When communicating with patients during the recruitment process, patients must be offered an opportunity to object before disclosing PHI with their family or friends.

Although some disclosures are not completely avoidable, such as visitors hearing a patient's name called out in a waiting room or a hospital patient in a 2-bed room possibly hearing a Jefferson community member speaking to the other patient, HIPAA requires reasonable steps to be taken to minimize these incidental disclosures.

- Before discussing patient information in person, ask the patient if it is okay to discuss information in front of the patient's family member or friend accompanying them. Alternatively, you can ask the family member or friend to leave, especially if the information is highly confidential.
- Speak in soft tones when discussing PHI in open areas such as the recovery room, emergency department, etc.
- Do not discuss PHI in public hallways, elevators or other public locations such as the cafeteria
- Use only the minimum necessary to minimize incidental disclosures.
- When calling patients, please verify the patient's identity before speaking. If the patient has a designated representative, ensure that the proper written authorization is on record to speak to that person.
- When leaving messages for patients such as voice or text messages, leave only the minimum amount of information needed. Do not leave patient diagnosis, medication or other clinical information on a patient telephone.

Transmitting Patient Information Electronically

Exercise precaution when electronically transmitting Jefferson e-PHI and other confidential information. All of Jefferson's information and data, in whatever form, must be afforded the highest level of protection and confidentiality. Jefferson has legal obligations for protection of its information and data.

- Documents electronically transmitted within the Jefferson network are secure. Documents electronically transmitted to any destination outside of Jefferson's secure campus network **must be encrypted.**
- To encrypt emails, include the word "secure" followed by a space at the beginning of the subject line of an email.
- Do not include PHI such as social security number, diagnosis, medical record number and other confidential information in the subject line of emails.
- Use of personal email accounts to transmit or store Jefferson related email is prohibited.

Mobile Devices

Jefferson community members should take all appropriate measures and precautions to safeguard, secure and prevent the loss, theft, damage, and/or unauthorized use of any Jefferson-owned or Jefferson-managed personal mobile device that contains Jefferson's confidential, proprietary and/or Protected Health Information.

- Keep all Jefferson-issued portable computing or mobile devices in a locked and secured environment when not being used
- Do not leave the computing/mobile device for prolonged periods of time in a vehicle, especially in extreme temperatures
- Do not leave the computing device unattended at any time in an unsecured location (e.g., an unlocked empty classroom or office)
- Keep the computing device in sight at all times while in public places, such as public transportation and at airports, restaurants, etc.
- **Immediately report the loss or theft of any Jefferson-owned or Jefferson-managed personal mobile device that contains Jefferson's confidential, proprietary and/or Protected Health Information to your direct manager or supervisor and IS&T Customer Service Center.**

Privacy Incidents and Breaches

A privacy breach is an impermissible acquisition, access, use or disclosure of PHI which compromises the security and/or privacy of PHI. Breaches pose significant financial, reputational or other harm to the affected individual(s) and to our organization. A privacy breach can be intentional or unintentional.

Examples of a privacy breach include:

- Lost or stolen laptop
- Stolen briefcase with documents containing PHI
- Disclosure of PHI without appropriate authorization
- Disclosure of PHI on social media
- Lost mobile device containing PHI
- PHI left in a public area
- Cell phone pictures
- Faxes sent to the wrong number
- Misdirected mail
- Inappropriately discarded PHI

Report all Known or Suspected Privacy Incidents

If you are aware that a breach or other privacy incident has occurred or suspect that someone violated the privacy and security of a patient confidential information, **you must immediately report it** to your supervisor, privacy officer or legal office.

Contact the Privacy Office at:

Privacy Office Hotline: 1-833-391-2547

Email: PrivacyOffice@jefferson.edu

You may file a confidential or anonymous report using the Jefferson Alertline:

1-888-5COMPLY (1-888-526-6759) or Jefferson.Alertline.com

Important General Privacy Safeguarding Tip Sheet

Jefferson takes the privacy and security of our patient information seriously! Members of the Jefferson community will be held responsible for any improper handling of confidential or Protected Health Information. Any member of the Jefferson community who violates the confidentiality of patients' Protected Health Information are subject to corrective and disciplinary actions, up to and including termination of enrollment.

The privacy and security of confidential and Protected Health Information starts with YOU!

DO:

- Secure information from improper disclosure
- Protect the integrity of the patient information and other confidential data
- Dispose of PHI in appropriate shredding bins
- Ensure the disclosure of information reached the intended person
- Secure workstations by locking or logging off of them
- Limit the use/disclosure of PHI to the "Minimum Amount Necessary"
- Keep the computing device in sight at all times while in public areas, such as on public transportation and at airports, restaurants, etc.
- Immediately report any known or suspected HIPAA/HITECH incidents

DO NOT:

- Access, use, or disclose confidential or Protected Health Information for personal gain! This includes, but is not limited to:
  - Posting to social media or contacting patients through social media
  - Contacting patients (or relatives or patients) via phone calls, text messages, letters, in-person communication or emails for purposes not related to your duties
- Leave a computing/mobile device for prolonged periods of time in a vehicle, especially in extreme temperatures
- Leave a computing device unattended at any time in an unsecured location (e.g., an unlocked classroom or office)
- Access PHI unless it is related to your job function or an authorized request
- Share PHI with family, friends or any unauthorized person

IMPORTANT!

The Jefferson community will be held responsible for any improper handling of confidential or protected health information. Any member of the Jefferson community who violates the confidentiality of patients' Protected Health Information is subject to corrective and disciplinary actions.