HIPAA Privacy & Security: What You Need to Know

Embrace Your Future

Providence

Providence

Table of Contents

Embrace Your Future

Privacy at Providence

The Health Insurance Portability and Accountability Act (HIPAA) and state and federal regulations must be followed by all Providence caregivers and workforce members.

HIPAA requires us to safeguard all healthcare information stored or communicated in any manner, whether oral, written, or electronic.

Viewing the records of family members and friends is prohibited unless you need the information to do your job, or you follow your department's procedure for appropriately obtaining access.

In any case, limit your use or disclosure of healthcare information to the minimum necessary, unless the information is needed by a provider to provide treatment to a patient.

Providence

HIPAA Privacy & Security: What You Need to Know

Providence

Members of the Providence St. Joseph Health (PSJH) workforce are expected to know and comply with privacy and security polices that govern the use of Protected Health Information (PHI). Workforce members should understand and comply with the following as it relates to these policies.

- *Never* view patient records outside your scope of work. Workforce members should only view records relevant to performing their job. No peeking! Even if the workforce member sees a neighbor, friend, or family member and are concerned about these patients, the concern does not give them the right to look at any patient files unless it is necessary for patient care, or for business -related purpose. **Unnecessarily accessing patient records is a violation of the patient's trust, our policies, and the law.**
- Workforce member should *never* share their ID or passwords with anyone and do not allow others to use the computer while they are logged in.
  - Workforce member should not leave their password written down near or on their computer.
  - Workforce members should make certain to lock or log off their computer when they step away.
- Understand what qualifies as protected health information (PHI). Examples of PHI include, but are not limited to:
  - Names and addresses
  - Telephone/fax numbers
  - Email addresses
  - Social Security numbers
  - Medical Record Numbers (MRN)
  - Dates that include Date of Birth, Death, Admission, Discharge
  - Full-face photos including masking and/or obscuring patient faces
- Use secure shred bins to dispose of documents containing PHI or other confidential information. Never recycle documents containing confidential information.
- Keep PHI out of sight and secure it when not in use to prevent unauthorized access.
- Avoid patient-related discussions in public areas and use discretion in shared patient rooms when discussing sensitive information.
- Workforce members are responsible for keeping health information received at work confidential. Do not post PHI to social networking sites such as Facebook, Instagram, Twitter, etc. This is a serious HIPAA violation and constitutes a breach.
- When sending a document or spreadsheet (attachment), ensure that the attachment has the minimum necessary information for the recipient of the attachment. Remove any sensitive information or PHI that is not needed prior to sending the attachment.

Last Updated May 2023

Risk and Integrity Services (RIS) Privacy

PHI is Protected Health Information or information typically associated with patients. Outside of direct treatment, PHI can only be accessed and used for minimally necessary purposed under the HIPAA Privacy Rules.

- Always use a cover sheet when transmitting information by fax.
  - Do not put confidential information on the cover sheet.
  - Include the sender's contact name and contact information in the event that the information is misdirected.
- Before discarding pill bottles, IV bags, vials, or other items with labels containing PHI, black out the information or remove the labels and dispose of them in the shred bin.
- Always verify patient identifiers prior to giving/sending patient-specific information to patients (e.g. AVS, prescriptions, requisitions, etc.), including to private addresses.
- Understand what constitutes a breach, and know how to report questionable events so they can be assessed in a timely manner by the RIS Privacy Office. A **breach** is defined as each individual instance of unlawful or unauthorized access to, use, or disclosure of a specific patient's medical information. Healthcare professionals that violate privacy laws and regulations, and commit a breach can face very serious consequences. These can include progressive discipline (up to and including termination). Healthcare professionals may also face criminal prosecution and civil penalties up to $250,000. The best way to prevent a breach is to always keep the information obtained at work confidential and follow proper security practices when dealing with PHI.
- Examples of potential breaches include, but are not limited to:
  - Viewing patient records without the "need to know"
  - Throwing PHI in the trash can instead of the shred bin
  - Giving discharge summaries and prescriptions to the wrong patient
  - Posting patient information/PHI to social networking sites or blogs
  - Sending faxes with confidential information to the wrong recipient
- Understand how to report a compliance issue or suspected breach:
  - Discuss the issue or concern with your immediate supervisor
  - Discuss the issue or concern with the department manager
  - Contact the Integrity Hotline at 888-294-8455, or Online or through the QR code. The integrity hotline is available toll-free 24 hours a day, 7 days a week. You may report concerns anonymously.
- Workforce member should consult PSJH's Code of Conduct when they have questions about doing the right thing. The Code will help them understand PSJH expectations and the importance of being honest and fair in all of our business interactions with customers, patients, members, payers, and vendors. The Code details how to report a violation or concern about potential illegal or inappropriate actions.
- Privacy & Information Security resources are available online.

Remember to always ask questions when you are in doubt!

Last Updated May 2023

Risk and Integrity Services (RIS) Privacy

Embrace Your Future

Privacy and SharePoint—What You Need to Know

Am I responsible for the data that I use and access on SharePoint?

- Yes. The data, whether PHI or PII, that you use in your job role must be safeguarded to ensure that other members of the workforce who do not need the information cannot access it.
- **Data that you put on SharePoint is your responsibility**. Any data, not just patient information, may be considered confidential and sensitive and must be safeguarded through the use of the appropriate SharePoint security controls which must be applied appropriately.
- You must be aware of the types of data that is in the documents that you post on SharePoint and who has access to this data as appropriate for business-related purposes.

What is PHI?

- PHI is Protected Health Information or information typically associated with patients
    - Outside of direct treatment, PHI may only be accessed and used for minimum necessary purposes under the HIPAA Privacy Rule
- PHI is not just clinical and diagnoses related information and may include things like name, Date of Birth (DOB), Medical Record Number (MRN), full or partial Social Security Number (SSN), Phone Number, Insurance Card Number (see full list on next page)

What is PII?

- PII is Personally Identifiable Information or information typically associated with any individual, which may include Providence caregivers
- PII may include, but is not limited to: Name, DOB, SSN (full or last 4 digits), Phone Number, Employee Information, Numeric Identifiers
- Some PII may be considered sensitive such as that relating to benefits, salary, employee actions, etc.

How do I safeguard data that I put on SharePoint?

- Determine whether the data that you are required to use in your role must be placed on SharePoint in order for you and/or others to perform your job. Consider what is minimally necessary. Data that doesn't need to be moved from one system to another shouldn't be (i.e. Epic data to SharePoint)
- Understand and utilize security settings appropriately
- Do not share documents on SharePoint with other members of the workforce who do not need access to the information
- Use caution when configuring settings that allow other individuals to share your documents. If you are the owner of a document, you should always be in control of who you share your document with

Embrace Your Future

HIPAA 18 Identifiers

- Name
- Address (all geographic subdivisions smaller than state, including street address, city county, and zip code)
- All elements (except years) of dates related to an individual (including birthdate, admission date, discharge date, date of death, and exact age if over 89)
- Telephone numbers
- Fax number
- Email address
- Social Security Number
- Medical record number
- Health plan beneficiary number
- Account number
- Certificate or license number
- Any vehicle or other device serial number
- Web URL
- Internet Protocol (IP) Address
- Finger or voice print
- Photographic image - Photographic images are not limited to images of the face.
- Any other characteristic that could uniquely identify the individual

Embrace Your Future

Impermissible Uses of Protected Health Information and the Electronic Health Record (EHR)

Risk and Integrity Services (RIS) Privacy

Searching for any individual, whether family (child, spouse, etc.), friend, co-worker, or member of the general public without a business reason (must be related to your Providence business role in the individual's treatment or payment for treatment). Accessing a record for reasons that are outside of your business-related function may result in disciplinary action including termination of employment. Access to the EHR is monitored on a 24/7 basis.

- Using patient (or co-workers/peers) chart for training purposes
  - There are test patients in the Epic Playground for training purposes
- Using the Electronic Health Record (EHR) to locate demographic information (i.e. personal service, social gathering, birthday, etc..)
- Searching for or reviewing for purposes of curiosity/concern about a co-worker, person of interest (people in the news, celebrities, etc.), family member or other individual's condition
- Using census boards/track boards or other modules in the EHR for purposes other than treatment of patients (making appointments for family, self or friends, how long the wait in the ED may be)
  - Accessing census boards and track boards are still access to patient records
- Circumventing hospital directory channels to locate family, peers, or friends in the hospital
- Circumventing requests for records (ROI) processes to obtain copies of medical records for self or others (including records needed for litigation, research, etc.)
  - Contact Health Information Management (HIM) for copies of medical records, or print through MyChart
- Using the EHR for employment-related action or investigation (i.e. to confirm whether an employee/peer was at a clinic appointment when they said they were)
- Sharing credentials or not logging off before workstation is used by another user
- Accessing the "appointment desk" to check appointment times for friends and family
  - Accessing the appointment desk is still accessing the EHR. The appropriate way to confirm an appointment is by contacting the clinic or as a MyChart Proxy
- Looking up a co-worker's information because they asked, and are not a part of the care team
- Monitor the care of a family member or co-worker, or look up test results
  - Requests for medical records can be made through HIM" similar to one above that references MyChart

This list is NOT all-inclusive of ways the EHR may be used inappropriately. For additional questions, please contact the Integrity Hotline at 1-888-294-8455 or ONLINE

Last Updated November 2023

Providence

Embrace Your Future

Patient Rights

Compliance Services

Doing the Right Thing Right: *Patient Rights to Request Changes to Their Medical Records*

Did you Know? Per Federal Privacy laws and Providence policy PSJH-RIS-850.07, an individual has the right to request Providence amend PHI or a record about the individual in a designated record set for as long as the PHI is maintained in the designated record set.

What does this mean? This means Providence needs to have a process where **the author** (of the medical information that is being requested to be changed) needs to **review** the request **and accept or deny**, in whole or in part, the requested changes no later than 60 days, or as required by law, after receipt of such a request.

a) If Providence grants the requested amendment, in whole or in part, it shall make the amendment and inform the individual.
b) If Providence denies the requested amendment, in whole or in part, it shall provide the individual with a written denial. Denied requests for amendments are also afforded an appeal process supported by the Health Information Management team.

Steps for Accepting the Amendment

1. Providence shall make the appropriate amendment to the PHI or record that is the subject of the request for amendment.
2. Within the required time limit, Providence shall inform the individual that the amendment is accepted.
3. Providence shall either comply with federal/state law requirements or make reasonable efforts to inform and provide the amendment within a reasonable time to the appropriate parties.

Remember: Providence is committed to upholding the rights of individuals with respect to PHI in accordance with HIPAA, other relevant laws, and Providence policies; and we rely on each of you to do your part.

Violations of policy can result in disciplinary action which may include termination of employment.
Rights of Individuals with Respect to Protected Health Information Standard

Embrace Your Future

A Duty to Report Potential Privacy Violations

Providence is committed to the highest standards necessary to secure the confidentiality, integrity and availability of our patients' protected health information (PHI). As such, caregivers and volunteers are required to report breaches of privacy or security, including inappropriate access to and unauthorized releases of patient PHI.

Any Providence caregiver who suspects a privacy or security violation, identifies an information security breach involving PHI, or recognizes a potential vulnerability that might compromise patient PHI should report such findings to any or all of the individuals identified below. This reporting requirement excludes permitted uses of PHI under HIPAA such as those necessary for "treatment, payment, and operations" (TPO).

To report a suspected privacy or security violation, please contact the Providence Integrity Hotline, 888-294-8455 or http://www.integrityonline.ethicspoint.com/.

Business Associate Agreement (BAA)

All BAA email communication will be directed to BAA@providence.org

Hands shaking

Kitterman, Jennie (she/her)
Senior Compliance Specialist

Embrace Your Future

HIPAA Privacy & Security: Recap for Students

Privacy Tips

TWO PATIENT IDENTIFIERS

Minimize searching for patients by name only. Utilize MRN or at least two identifiers to locate the record. Refer to your preceptor or local nursing policies.

BUSINESS RELATED ACCESS

Only search for and access patient information (including demographic information such as name and address) that you have a need to access in the scope of your training. Demographic information is Protected Health Information.

KEEP CREDENTIALS SECURE

Do not share your credentials with anyone—including other students. Do not use the credentials of others. What is accessed under your credentials is your responsibility.

ACCESS IS MONTORED

Your access to the electronic health record (EHR) system is monitored 24/7 through an automated monitoring system. Impermissible access will result in disciplinary action.

HOW DO I REPORT A CONCERN?

- Inform your direct supervisor or department core leader
- Call the Integrity Hotline: 1-888-294-8455
- Report online

All reports are treated ***confidentially***!

Last updated May 2022

Providence

Risk and Integrity Services—Privacy

Embrace Your Future

FAQ

Question:

Can we access our medical records once we are in rotation?

Answer:

Using a formal process (above), you can view your medical records. But you are not permitted to lookup your own medical record when logged into the electronic medical record.

Embrace Your Future

Embrace Your Future

Thank you for completing your HIPAA training

As a part of your student clearance processed, you will need to sign the Confidentiality and Nondisclosure Statement, ***this is a requirement to starting your rotation.***