HIPAA Privacy & Security: What You Need to Know

Providence expects that all workforce members and those with access to our electronic health records will protect our patients’ information in accordance with the HIPAA privacy and security rules and applicable state laws. This tip sheet highlights key HIPAA focus areas. In a time of increasing government enforcement, fines and potential jail time, these tips will help you do the right thing.

- Never view patient records outside your scope of work. Only view records relevant to performing your job. No peeking!
- Never share your ID or passwords with anyone and do not allow others to use the computer while you are logged in. Don’t leave your password written down near your computer. Make certain to lock or log off your computer when you step away.

- Understand what qualifies as protected health information (PHI). Examples of PHI include:
  - Names and addresses
  - Telephone/Fax Numbers
  - Email Addresses
  - Social Security Numbers
  - Medical Record Numbers
  - Dates that Include Dates of Birth, Death, Admission, Discharge
  - Full-Face Photos and Comparable Images of Patients

- Providence has well defined processes for accessing one’s health record that must be followed by all patients – including patients who are also employees, medical staff, volunteers and others with access to Providence systems and paper records. Providence policy does not permit physicians, other care providers or physician practice staff to access their own or their family members’ PHI through the electronic health record. All access to PHI must be requested through official channels in the same way that any other patient obtains access. Note that Providence policy may be different from that of other covered entities for which you provide care.

- Use secure shredder 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.
• You are responsible for keeping information received at work confidential. Do not post PHI or other confidential information to social networking sites such as Facebook or Twitter. This is a serious HIPAA violation and constitutes a breach.

• Always use a cover sheet when transmitting information by fax. Do not put confidential information on the cover sheet.

• 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 shredder bin.

• Understand what constitutes a breach. A breach is defined as the unauthorized acquisition, access, use, or disclosure of PHI which compromises the security or privacy of the 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 breaches include:
  ▪ Viewing patient records without the “need to know”
  ▪ Throwing PHI in the trashcan instead of the shredder 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:
  1. Discuss the issue or concern with your immediate supervisor
  2. Discuss the issue or concern with the department manager
  3. Contact your local or regional compliance or privacy representative
  4. Call the Providence Integrity line at (888)294-8455. The Integrity Line is available toll-free 24 hours a day, 7 days a week. You may report concerns anonymously.

• Consult Providence’s Code of Conduct when you have questions about doing the right thing. The Code will help you understand Providence 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. Copies of the Code in different languages can also be found online.

• In addition to the Code of Conduct, Providence policies on Conflict of Interest, Fraud & Abuse, Vendor Relations, Non-Retaliation and Confidentiality are available on Providence’s internet site at www2.providence.org/phs/integrity/Pages/default.aspx.

  Remember to always ask questions when you are in doubt!
HIPAA Privacy & Security

Learning Objectives

- Understand how HIPAA applies to your new role at Providence
- Understand and commit to Providence Privacy standards
- Understand and commit to Providence Security standards
- Learn where to go to ask questions and report concerns
What is HIPAA?

- The federal statute that regulates the confidentiality, integrity and availability of patients’ Protected Health Information (PHI)
- Identifies 18 elements of PHI
- Applies to all written, verbal and electronic information

What is PHI?

Protected Health Information (PHI)
- Names
- Social Security Number
- Medical Record Number
- Geographic location smaller than state
- AI dates except for year
- Biometric ID-fingerprint, voice, etc.
- Health Plan number
- Account number

- License number
- Age, less than 90
- Phone number
- Fax number
- Email address
- Vehicle Identification
- Device numbers
- URL
- IP address
- Full face images
- Any other unique identifying number, characteristic, or code
Minimum Necessary Requirement

- We do not access, use, disclose or discuss patient-specific information with others unless:
  - Necessary for treatment, payment, or operations
  - Required by law, or
  - Authorized by patient

Access or disclose only the minimum information needed to do your job.

While you are at Providence:

- Access is granted only for business reasons

- **You may not** access your own health care record, or that of family members, friends, coworkers, or neighbors

- Access is monitored and recorded

- Inappropriate access, use, or disclosure will result in corrective action
HIGHTECH

HIGHTECH Act – Health Information Technology for Economic and Clinical Health Act of 2009

- HITECH was enacted to stimulate the adoption of electronic health records (EHR)
- Widens the scope of privacy and security protections available under HIPAA
- Increases the potential legal liability for non-compliance
- Provides for more enforcement of privacy breaches

Privacy & Security Breaches

A breach is theft, loss, and inappropriate use or disclosure of PHI, including:
- Paper documents containing PHI disclosed to unintended recipients
- Stolen or lost laptops, flash drives, phones, or any other personal electronic device
- E-mails or faxes sent to an unauthorized party
- Unencrypted electronic information sent outside the Providence network
- Unauthorized access (e.g. "peeking")
- Saving a file containing PHI to a widely accessible storage location
Social Media Sites

- HIPAA rules also apply in social media settings
- Never post PHI (including photos) to a social networking site
- Sanctions can even be imposed to posts that share confidential, or proprietary information, photographs or videos about Providence

Refer to Providence Policy PROV-COMM-604

Reporting a Breach

Immediately report any compliance concerns and potential breaches to your manager, the Compliance office, or the Integrity Line

- Compliance Office: (503)574-9686
- Integrity Line: (888)294-8455
Office for Civil Rights Enforcement

Four tiers of penalties for breaches that reflect increasing levels of culpability with corresponding monetary penalties:

- Inadvertent disclosures
- Reasonable Cause
- Corrected Willful Neglect
- Uncorrected Willful Neglect

State Attorneys General may bring civil actions against violators (individual and organizational)

Privacy Best Practices

Our expectation while you are at Providence:

- Never view patient records outside of your scope of work—No peeking!
- Use secure shredder bins to dispose of documents containing PHI—Do not recycle!
- Keep PHI out of sight and secure when not in use
- Avoid patient-related discussions in public areas
Security Best Practices

- Secure your computer, voicemail and other passwords—lock and don’t share!
- Use your Providence email account for communications related to your learning activities—never use a personal email account!
- Never download confidential information onto a home or non-Providence device
- Store portable devices and other electronic media in a secure location—your car is not a secure location!

Confidential Information

You are also expected to protect confidential information

- Includes confidential information about
  - Patients and Members
  - Employees
  - Students
  - Residents
  - Business operations not available to the public
- Removing confidential information from work location and requires supervisor approval
Questions?

- Security Questions:
  Oregon Region Security Analyst
  Greg Chupp
  (503)893-7169
  Greg.Chupp@providence.org

- Integrity, Compliance & Privacy Questions:
  Compliance Office
  (503)574-9886
  Integrity Line
  (888)294-8455

- Email or Computer Access Questions:
  IT Help Desk
  (503)216-2800
  OR Intranet site under Resources

We Are All Responsible

"No snowflake in an avalanche ever feels responsible." — Voltaire