

Privacy and Security

Presented by
PSJH Risk & Integrity Services, Compliance

Our Commitment to Patient Privacy



- PSJH has an obligation to safeguard patients' health information
- HIPAA/HITECH applies to all written, verbal and electronic health information
- All workforce members need to know what protected health information (PHI) is and how to use it

Protected Health Information: 18 Identifiers

- Names
- Social Security Number
- Medical Record Number
- Geographic location smaller than state
- All dates except for year
- Biometric (ID-fingerprint, voice, etc.)
- Health Plan number
- Account number
- License number
- Age, over 90
- Phone number
- Fax number
- Email address
- Vehicle Identification
- Device numbers
- URL
- IP address
- Full face photographs
- Any other unique identifying number, characteristic, or code

HIPAA Privacy Rule: Permitted Uses and Disclosures



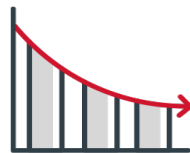
Treatment

- Access EMR to treat patient
- Share PHI with other providers of the patient
- Share PHI for consults and referrals
- Share PHI with pharmacies



Payment

- Share PHI with insurance organizations
- Share PHI with family members to obtain insurance or other payment information
- Share PHI with collections agencies to obtain payment



Operations

- Use PHI for quality/safety improvement
- Use PHI for administrative/legal purposes
- Use PHI for auditing and compliance investigations

Uses and Disclosures permitted without written patient authorization

Using PHI for Treatment

You may use and disclose PHI to provide the patient with appropriate treatment and may disclose PHI to other health care providers that have a care relationship with the patient—including nurses, labs, technicians, etc.

PHI may not be shared with providers who are not involved with the patient's care.

Caregivers may not share PHI with other caregivers, unless it is necessary for on-going care or in a legitimate educational setting.

A former care relationship, curiosity, or personal relationship, does not always qualify as involved with the patient's care.

What Can You Disclose to Others?

When the patient is present and has the capacity to make decisions:



You may discuss the patient's health information with a family member, friend, or other person if the patient agrees or, when given the opportunity, does not object



Only disclose information that the person involved needs to know for that episode of care—**Minimum Necessary**

When the Patient is Incapacitated

When the patient is unable to give authorization due to incapacity or other emergency circumstances:



Check the chart for any patient preferences regarding others involved with their care



You may share the patient's information with family, friends, or others, as long as you determine, based on professional judgment, that it is in the best interest of the patient



Only disclose the information the person involved in care needs to know about the patient's care

Access to Epic and Other Information Systems

Access is granted only for business reasons per the Acceptable Use Agreement

Access is monitored and recorded

You may not view **your own record**, or information of family members, friends, neighbors, or co-workers



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

Refer to Providence Policy PROV-PSEC-802

Privacy Safeguards: What Should You Do?



Never use patients' names, or other elements of PHI, in hallways, elevators, or other public areas.



Speak quietly when discussing patient information in reception areas, or other areas where conversations may be overheard.



Keep all papers with PHI out of view of the public.



Dispose of paper with PHI in designated bins.



Always use a fax coversheet

Security Safeguards: What Should You Do?



Store portable devices and other electronic media in a secure location—your car is not a secure location!



Never download confidential information onto a home or non-Providence device.



Only use your Providence email account—never use a personal email account to send assignments or other Providence related work product.



Secure your computer, voicemail and other passwords—lock and don't share!

Taking Photos

Photographs and or videotape may be taken to assist in patient care and treatment when it may be of benefit to the patient's plan of care.



Photography/videography may not interfere with the provision of patient care.



Images used for medical education, staff education or public relations require authorization.



You may not use your cell phone or any other personal image taking devices.

Refer to Photography/Videography Policy & PROV-PSEC-803

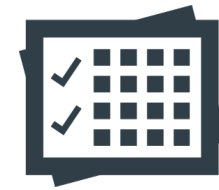
Responsible Use of Social Media



HIPAA rules also apply in social media settings



Never post PHI (including photos), confidential, or proprietary information to a social networking site



Sanctions may be imposed for any posts that violate the Social Media policy

Refer to Providence Policy PROV-COMM-604

Your Ethical Duty to Report

IMMEDIATELY



Report all privacy concerns or incidents to your manager

Or contact the 24/7 PSJH Integrity Hotline at (888)294-8455, or
submit a report online at

<http://www.integrityonline.ethicspoint.com/>