Compliance, Privacy, and Security

Code of Conduct

Our organization's Code of Conduct (COC) provides us with a set of standards that guides our decision-making and our commitment to "doing the right thing right". The COC should be used as a reference document for conduct guidance. It is always available on our Intranet and Internet.
The COC is also available in hardcopy in your orientation packet. ENGLISH SPANISH

Compliance Liaisons

We have compliance representation in each region and each ministry has an assigned compliance liaison to assist you with any questions or concerns you might have. Please review the list HERE. This list is also available in hardcopy in your orientation packet.

Records Accuracy and Retention

- We prepare and maintain accurate and complete documents and records. Altering or destroying records is prohibited.
- Records include: financial records, claims made for payment, patient records, employee timesheets and expense-related forms.

Gifts and Entertainment

Accepting gifts and offers of entertainment creates a risk that our judgment and decisions can be influenced.

- Tickets to events, cash, gift cards and gift certificates may ***only*** be accepted when given to you by your organization or a fellow caregiver.
- Accepting a modest, perishable gift from a vendor or non-employed provider that is shared among co-workers (i.e. fruit basket, box of chocolates, donuts, bagels, pizza, etc.) is acceptable.

Federal and State Health Programs

- Providence is committed to full compliance with laws and regulations relating to:
    - Fraud, Waste and Abuse (FWA) Prevention
    - False Claims Act (FCA)
        - Claims for payment are expected to be accurate and represent the services actually provided
    - Patient referrals
    - Providing medically necessary services (EMTALA)
    - Medicare's Conditions of Participation
    - Submission of cost reports and other requirements

HIPAA and Protected Health Information (PHI)

Safeguarding Patient Information

It is everyone's responsibility to safeguard Protected Health Information (PHI) including that which is in paper, electronic and verbal formats.

All individually identifiable information (including demographic data) must be safeguarded and consists of information that relates to:

- the individual's past, present or future physical or mental health or condition,
- the provision of health care to the individual, or
- the past, present, or future payment for the provision of health care to the individual,
- and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual

Use of patient information

There must be a legitimate and job-related reason for looking at patient information. When using patient information for payment or internal health care operations activities, only that which is the *minimum necessary* to

complete the job related task should be used. Volunteers and other workforce members may have access to written or electronic patient information depending on the duties performed. Those who deliver mail or flowers will know the patient's name and room number. Those who work the Admitting Desks or Surgery Waiting Desk may learn/know more details of a patient's care/situation. Those at the Front Desk will have access to the names and room numbers of all inpatients who have chosen to be listed in the Directory as well as certain outpatients undergoing procedures. Some Volunteers will meet with specific patients having a particular diagnosis as part of structured support programs such as Mended Hearts. It is important that the information that you are entrusted with to perform your job is only used for this purpose and not further disclosed to others who do not need to know this information.

All information related to any patient at any health care facility is confidential. *The very fact that a person is receiving health care services or that a patient was discharged on a specific date is confidential even when no other information regarding the person's condition or treatment is revealed.*

Federal and state laws govern when and how we may release information about patients.

Written information on patients

- Lists of patients, patient labels, patient reports or notes from patient conversations should be handled cautiously when used internally and never taken out of the facility.
- Papers with patient information intended to be discarded should be placed in a secure shredding bin. These include large locked gray garbage cans with slots in the lids. Paper placed in a shredding container may not be removed and re-used for any purpose.
- Patient census lists, visitor log books and other paper with patient information should never be left where the general public can see the contents. Census lists and log books maintained in the Admitting Desks and Surgery Waiting Room desk must be placed out of sight in a locked drawer if the area is to be left unattended.

Computer systems

If your duties require you to use a computer, you must be given a user ID and password. The ID and password is your electronic signature in the system.

- Never give your password or credentials to anyone – not even a member of the Information Services Department – or use those of anyone else.
- If you must write down your User ID and password to remember it, keep the information in your wallet but without any reference to what the information is.
- Always lock or log off the computer you are using before you walk away – even for a short period.
- Know the location of the printer you are sending a print job to and remove it right away.
- Be aware of persons who may attempt to read confidential information over your shoulder.
- Never allow someone else to work under your ID and password.
- Access to all electronic health records is monitored to safeguard patient privacy and ensure integrity of protected PHI.
- It is against policy to access any record without legitimate business need which includes but is not limited to your co-workers, friends, family members', or your own.
    - Inappropriate access, use or disclosure will result in corrective action up to and including termination.

The Directory

The Directory is a list of patients. Patients at the hospital are asked at the time of admission if they want to be listed in the Directory. When a patient chooses to be listed, the patient's room number and general condition (good, fair, guarded, poor) can be given to callers who ask about the patient by name.

Patients sometimes don't want to be listed in the Directory. Patients who choose not to be listed are told to notify their family members or friends of their room number since this will not be given out by the Operator or Information Desk. Visitors who ask about an unlisted patient at the Information Desk will be told by the Information Desk that

there is no patient by that name" Mail sent to unlisted individuals is marked "return to sender".

Volunteers or other workforce members who are stopped by visitors and asked patient location information must redirect visitors to the Information Desk.

Talking about patients
Public areas such as elevators, cafeteria, gift shop and patient waiting areas are not appropriate areas for talking about a patient. Caution must be used in shared rooms that may involve pulling a curtain between the beds as a reasonable privacy barrier. If a conversation will occur between a caregiver and a patient in a shared patient area, caution should be used to ensure that information, particularly that which is sensitive, is reasonably safeguarded from impermissible disclosure to another patient who may be sharing a room. If in doubt, talk to your supervisor.

Discussions of the patient with others

- **Discussion of the patient with the patient's family, friends and other visitors**: Generally, it is the patient who controls what information is shared with the patient's visitors. When the patient cannot make this decision due to incapacity, his or her treatment team will use their professional judgment to share what is in the patient's best interests with the patient's visitors. When visitors ask questions about an incapacitated patient, it is always appropriate to redirect them to the patient's treatment team>**Discussion of the patient's care with members of the patient's treatment team:** It is acceptable that a patient's treatment team, including physicians, nurses, therapist, etc. will have access to information necessary to provide appropriate treatment to the patient.

- **Discussion of patients with staff members who are not involved treatment of patient**: Persons not involved in the direct treatment of a patient should not use or disclose that patient's information except as minimally necessary in order to perform the functions of their role. While Environmental Services or Facilities and Maintenance may require no access to patient information, other service lines such as those that support payment functions will need certain patient information to perform their role.

Rights of Patients

All persons have certain rights with respect to their health information. Those rights are summarized below as set forth in the organizations Notice of Privacy Practices.

- **Right to inspect and copy records**
  All persons have a right to examine and copy their medical records, billing records related to health care and other records that make up their complete health record or "designated record set."
- **Right to restrict uses and disclosures**
  All persons have a right to request that we not use their information for certain purposes or share their information with others they identify.
- **Right to receive information in a confidential manner**
  Patients may ask that we send records or call them at locations other than their primary residence in order to assure greater confidentiality of their information. Do not leave phone messages with patient information on answering machines or with another person without patient permission.
- **Right to an accounting of certain disclosures**
  Patients have the right to request a list of certain disclosures that we are permitted by law to make without their request.

Security of Confidential Information

- Confidential information includes - information about patients, caregivers, students, residentsor business operations that is not available to the public
- Do not remove information unless you have received approval from your manager. If you are authorized to remove information from the premises, understand the policies that apply transmission of such information.

- **Tips:**
  - Remember that use of organizational assets such as computers is not private and may be monitored at any time.
  - Use approved applications to access organizational information remotely
  - Protect your computer by contacting your service desk to download any software
  - Obtain management approval to use personally owned devices
  - Do not send patient or confidential information to a personal (non-business) email address
  - If you have permission to transmit patient or confidential information outside of the organization email domain ensure that you apply encryption technology
  - If you must text in an emergency situation, only provide the minimum necessary PHI
  - Always use shredder bins to dispose of confidential information
  - To avoid phishing schemes, do not click on suspicious links and know how to report them to Information Security.
  - Only authorized members of the workforce should be accessing secure areas by way of their own badge.

Acceptable Use of Information and Information Systems

Social Media Use

- Social media use information is available in the *legacy PHS policy PROV-COMM-604* or the *legacy SJH policy SO-HR-225*.
- **Individuals** can be held *personally and legally* responsible for their publicly made opinions and comments– this includes personal social media sites.

Reporting Potential Wrong Doing

Every caregiver has a responsibility to report potential wrongdoing.

- Our compliance program relies on caregivers at the ministries informing us when things do not seem to be in alignment with our Mission, Values, Vision, Promise, policies or Code of Conduct.
- PSJH's Non-Retaliation policy protects caregivers from harassment or other adverse actions for reporting potential wrongdoing in good faith.
- If you ever feel like someone is retaliating against you for reporting a concern, you should report this to RIS-Compliance or your local compliance/privacy representative.

What to Report

- Inappropriate access or disclosure of protected health information
- Code of Conduct or Compliance and Privacy Policy violations
- Misuse of social media
- Fraud and abuse concerns
- Billing and coding errors

How to Report Concerns

- Discuss the issue or concern with your supervisor;
- Discuss the issue or concern with the department manager;
- Contact compliance liaison
- Call the Integrity Hotline (888-294-8455) or use Integrity Online, our web-based reporting tool.