



# Integrity, Compliance, Privacy and Security



# Objectives

---

- Code/Standard of Conduct
- Compliance Program
- Reporting Process
- Your Commitment



# Code/Standard of Conduct

---

- Provides us with a set of standards that guides our decision-making and our commitment to “doing the right thing right”.
- Reflects our Mission, vision and core values.
- Describes on paper the expectations for compliant behavior.
- Should be used as a reference document for policies and government guidance.
- Available online on our Intranet and Internet.



# What is Compliance?

---

Compliance is knowing and following the ethical, legal and policy requirements that apply to your job to reduce the risk of fraudulent or abusive practices.



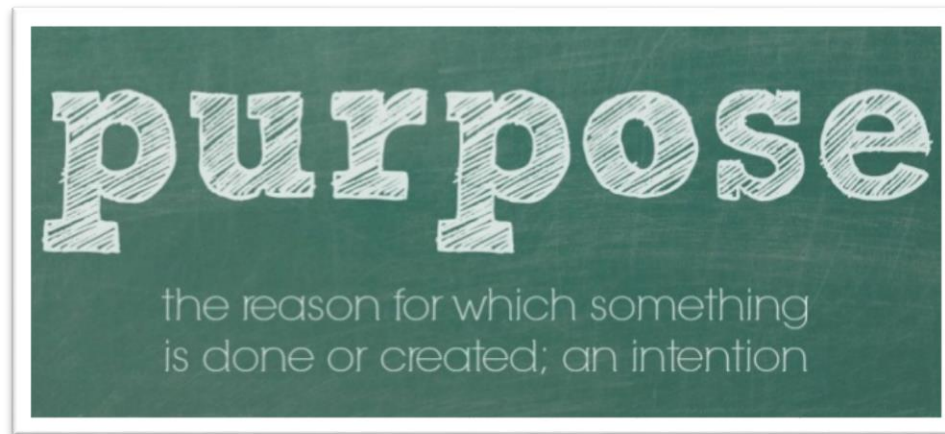
Compliance is a prevalent business concern, partly because of an ever-increasing number of regulations that require companies to be vigilant about maintaining a full understanding of their regulatory compliance requirements.



# Compliance Program- Our Purpose


---

- To maintain the integrity of the heritage and tradition of our organization by following the ethical commitments, laws, rules and regulations that govern our business conduct.
- To support **YOU** in “doing the right thing right”.
- To protect Providence St. Joseph (PSJH) Health from risk.



# Compliance Program- Education

---

- **Mandatory** compliance education is automatically assigned to your HealthStream account on your start date. 
- All caregivers receive the Core Compliance and Privacy & Security education.
- Due within **30 days of date of hire.**
- When necessary, other forms of education will be provided in your area or made available and communicated out appropriately.



# Compliance Program- Healthcare Laws

- Fraud, Waste and Abuse (FWA) Prevention
- False Claims Act (FCA)
- Anti-Kickback Statute (AKS)
- Stark Law
- Records Retention

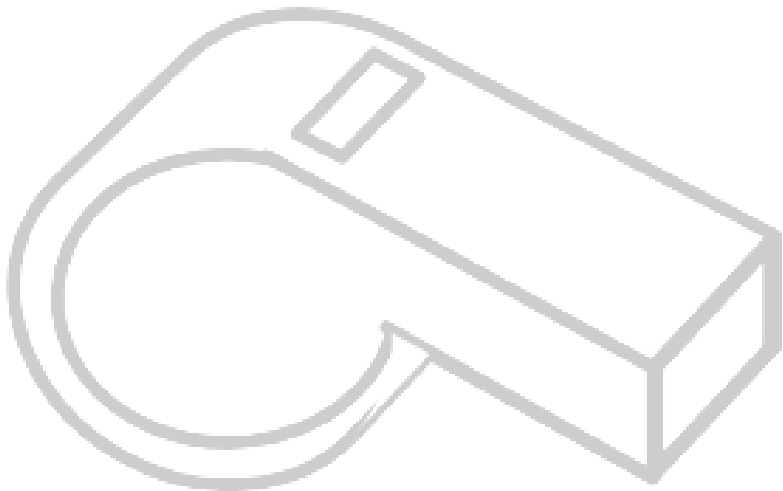




# Compliance Program- Whistleblower Protections

---

- A person who knows an FCA, AKS, Stark or any other type of violation has occurred and feels the organization is not correcting the issue may file a lawsuit on behalf of the government.
- If the case is successful, the whistleblower (person who reported the violation) may share in the recovery amount.
- Federal and state laws protect whistleblowers from threats, harassment and retaliation.





# Compliance Program- Conflicts of Interest

---

- Conflicts of Interest (COI) may occur when personal/outside interests or activities influence or appear to influence our actions and decisions regarding job-related duties.
- Avoid activities and relationships that may impair our independent judgment and unbiased decision-making.
- Information gained from our jobs/positions are not to be used for personal gain or advantage, or to assist others, including family members, in profiting in any way at the expense of the organization.



# COI- Caregiver Responsibilities

- All caregivers have the responsibility to disclose a potential conflict of interest to their manager as soon as the situation arises.
- Directors and above are automatically assigned a COI Disclosure form online and is required to be completed annually.
- Be aware of our Conflicts of Interest policy and *when in doubt, ASK!*



# Compliance Program- Gifts & 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 very modest, perishable gift that may be shared among co-workers, like a fruit basket or a box of chocolates is OK.



# Harassment and Workplace Violence

- “Zero-tolerance” policy.
- Report intimidating or disruptive conduct by or against individuals, including physicians.
  - This may include language, documents, “jokes”, cartoons, behavior and more.
- PSJH prohibits any action against any workforce member for reporting concerns in good faith or who assists in the investigation of a concern.



# Compliance Program- Privacy

---



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

- PHI consists of 18 identifiers that can be used to identify an individual that was created, used or disclosed in the course of providing healthcare services.
- Only access and/or disclose the *minimum necessary* PHI you need to do your job.
- There must be a legitimate and job-related reason for looking at patient information.



# Compliance Program- Privacy: Social Media

---

- Social Media guidelines are available for you via the PROV-COMM-604 policy.
- Confidential, or proprietary information, photographs or videos about our patients are not to be shared on personal social media sites.
- **Individuals** can be held *personally and legally* responsible for their publicly made opinions and comments– this includes personal social media sites.



# Compliance Program- Privacy: Media Inquiries

- Politely decline to make comments to any media inquiries.
- Notify your supervisor.
- Direct all media inquiries or requests to use the PSJH logo to the Marketing and Communications Department.





# Compliance Program- Privacy: PPM

---

The Proactive Privacy Monitoring program monitors access to all electronic health records (EHR) to safeguard patient privacy and ensure integrity of protected PHI.

- It is against Providence St. Joseph Health policy to access any record without legitimate business need which includes your co-workers, friends or family members’.
- Inappropriate access, use or disclosure will result in corrective action up to and *including termination*.



# Compliance Program- Privacy Breaches

---

A breach is the acquisition, access, or use of PHI in a manner that is not permitted by HIPAA and compromises the security or privacy of the PHI.

- Stolen or lost laptops, flash drives, phones, or any other personal electronic device
- E-mails or faxes sent to an unauthorized party
- Unauthorized access (e.g. “peeking”)

Report all potential breaches to your manager and local privacy office immediately.



# Compliance Program- Security: Best Practices



- Keep all work passwords private and secure and do not share with anyone.
- Lock or log off your computer when you leave your workstation.
- A vehicle is not considered a secure location and should not be used to store confidential information, mobile computing or storage devices.
- Double check fax numbers and use a cover sheet when faxing.
- Use #secure# in your subject line when sending confidential information outside of the organization.



# Compliance Program- Security: Best Practices

---

- Do not send confidential information to a personal (non-business) email address.
- Texting is not secure. 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.
- Only PSJH caregivers should be accessing secure areas. Watch for tailgating.



# Compliance Program- Security: Acceptable Use

---

- Remember that computer and internet usage is not private and is considered property of PSJH and may be viewed or monitored.
- Use approved applications to access PSJH information remotely.
- Protect your computer by contacting your service desk to download any software.
- Obtain management approval to use personally owned devices to conduct PSJH business; they must be encrypted and password protected.



# Government Requests

---

- Contact your supervisor and your region compliance office as soon as possible if approached by a government agent in person or by phone.
- Be polite to the agent.
- PSJH will cooperate with requests from government agencies.
- Responses will be clear and truthful.
- No alteration or destruction of records will occur.



# EMTALA

---

EMTALA is the Emergency Medical Treatment and Active Labor Act (1986). EMTALA requires Medicare-participating hospitals (including Critical Access) to provide:

1. Medical screening examinations to any individual who (regardless of insurance or ability to pay):
  - Presents to the Emergency Department (ED), including Labor & Delivery and psych intake-assessment areas.
  - Is outside the ED but on hospital property
  - Is not on hospital property but in a hospital-owned and operated ambulance
  - Is in a non-hospital-owned ambulance that has arrived on campus
2. Stabilizing treatment for emergency medical conditions.
3. Appropriate transfers to hospitals with specialized capabilities for stabilizing treatment.

When patients are on the hospital property (within 250 yards of the ED), ask for help and if it is evident they need screening for an emergency medical condition, our obligation is to ensure they arrive at our emergency department.

*Never delay care to obtain insurance information and never answer insurance related questions unless trained to do so.*





# Compliance Program- Reporting Potential Wrong Doing

---

## Every caregiver has a responsibility to report potential wrongdoing.

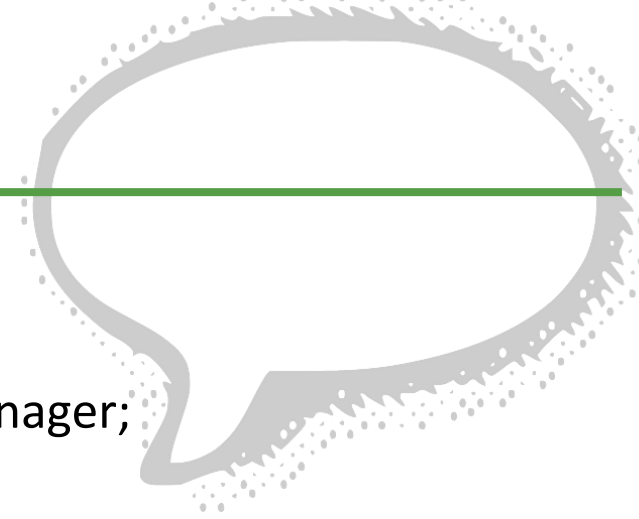
- Our compliance program relies on caregivers at the ministries informing us when things do not seem to be in alignment with our Mission, core values, policies or Code/Standard of Conduct.
- PSJH's Non-Retaliation policy protects caregivers from harassment or other adverse actions for reporting potential 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.



# How to Report Concerns

---

- Discuss the issue or concern with your supervisor;
- Discuss the issue or concern with the department manager;
- Contact RIS-Compliance or your local compliance/privacy representative; or
- Call the Integrity Hotline **(888-294-8455-PHS)** or use Integrity Online, our web-based reporting tool.



# What to Report: Potential Wrongdoing

---

- 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.



# Your Compliance Team

---

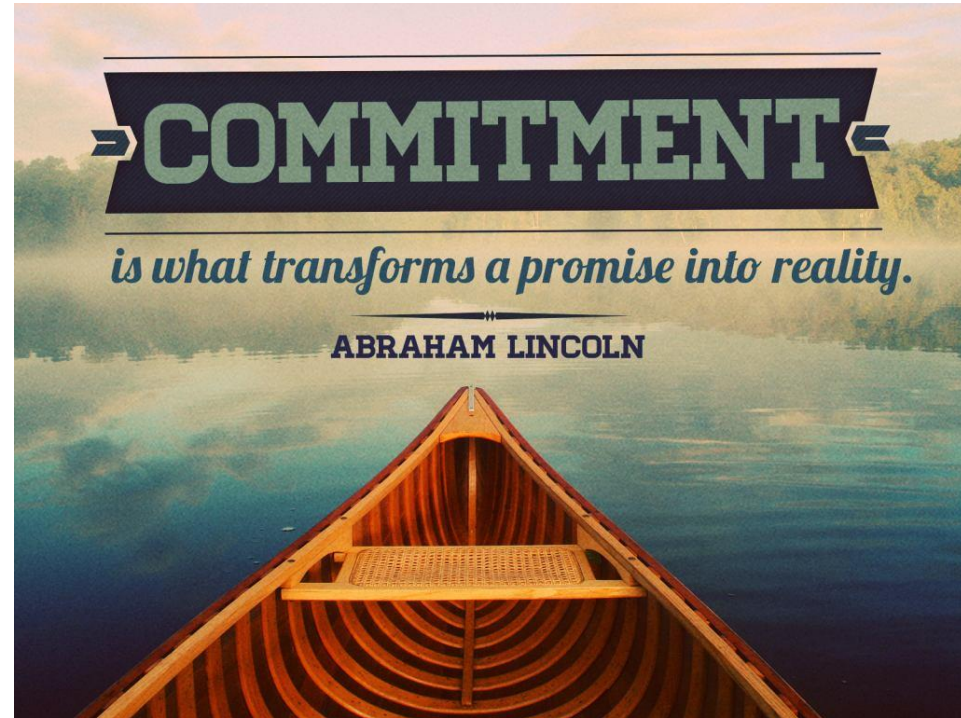
- **Senior Director Audit/Compliance**
  - Pat Cessnun- 425-254-5326
- **Compliance/Privacy Program Manager**
  - Stephanie Tasker- 907-212-3077
- **Information Security**
  - Jyl Swegle- 907-212-7939



# What YOU Committed To...

---

- Code of Conduct Acknowledgement
- Acceptable Use Agreement
- Confidentiality Agreement



*Thank you*

