

Providence Regional Medical Center Everett (PRMCE) Quality & Safety

The following are excerpts from employed caregiver annual courses provided to students and learners for onboarding compliance

Protected Health Information: 18 Identifiers

The following are considered identifiers under HIPAA:

1. Names
2. Geographic subdivisions smaller than a state (address, zip code, etc.)
3. All elements of dates (birth date, admission date, discharge date, date of death)
4. Telephone Number
5. Fax numbers
6. E-mail address
7. Social security numbers
8. Medical record numbers
9. Health plan numbers
10. Account numbers
11. Certificate/License number
12. Vehicle numbers
13. Device identifiers and serial numbers
14. Web Universal Resource Locators (URL)
15. Internet Protocol (IP)
16. Biometric Identifiers (fingerprint, voice)
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code (tattoos, birthmarks, scars, initials, tax ID #)



Use and Disclosure of Protected Health Information (PHI)

Workforce members 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 - includes nurses, labs, technicians, etc. Only minimal necessary information may be used or disclosed for healthcare operations and payment related functions. A patient's prior written authorization is generally required for other uses and disclosures beyond treatment, payment and healthcare operations.

Select the buttons below for examples.

**Examples of appropriate
sharing with others**

**Examples of inappropriate
sharing with others**



Use and Disclosure of Protected Health Information (PHI)

W
d
la
o
o



Examples of appropriate sharing with others:

- A caregiver may use discretion and discuss a patient's treatment in front of the patient's friend if the patient asks that her friend come into the treatment room.
- A caregiver may discuss the after-care plans with a patient with an individual who has accompanied the patient to a medical appointment. The information must be "need to know" for the person supporting the patient.
- A doctor may give information about a patient's mobility limitations to the patient's sister who is driving the patient home from the hospital.

Use and Disclosure of Protected Health Information (PHI)

W
d
la
o
o



Examples of inappropriate sharing with others:

- PHI may not be shared or spoken with providers who are not involved with the patient's care.
- The use of personal devices to take or share pictures or videos with other caregivers is prohibited even if the image is believed to be de-identified.
- A former care relationship, curiosity, or personal relationship, does not always qualify as involved with the patient's care.

Other Information that Must Be Safeguarded

Workforce members are expected to protect business confidential Information, which may include but is not limited to the following:

- Employee/Personnel information (includes, students, residents, volunteers)
- Employee Health information
- Business operations not available to the public
- Board, Medical Staff Committee, etc. meeting minutes, notes or actions
- Trade secrets or other confidential information/processes
- Privileged information from internal/external counsel
- Visitors (could be Protected Health Information)



Access to Epic and Other Information Systems

Can I access my family, friend or co-worker's medical record?

Can I access my own medical record?

Is EHR access monitored?

Can I be terminated for inappropriate access, use or disclosure of PHI?



Federal law and Providence only allow access to a patient's medical record for treatment, payment, and healthcare operations purposes. If you are not part of the care team, you may not access a patient's medical record for any reason. There are no exceptions to this for family, friends, or co-worker or because someone requested that you access their record but you are not involved in their care as a Providence workforce member.

Access is granted based on job role and is monitored and recorded 24/7

Access to Epic and Other Information Systems

Can I access my family, friend or co-worker's medical record?

Can I access my own medical record?

Is EHR access monitored?

Can I be terminated for inappropriate access, use or disclosure of PHI?



Providence policy prohibits workforce members from using their work provided credentials to access their own medical record within the electronic health record (EHR).

Workforce members must request access and/or copies of their medical records the same way any other patient would through the patient portal or by contacting HIM/medical records or their physician's office.

Access is granted based on job role and is monitored and recorded 24/7

Access to Epic and Other Information Systems

Can I access my family, friend or co-worker's medical record?

Can I access my own medical record?

Is EHR access monitored?

Can I be terminated for inappropriate access, use or disclosure of PHI?



Providence monitors workforce member access to the EHR system 24/7 . Suspicious access is investigated. This includes but is not limited to access to ED track boards, census lists, etc. It is all PHI!

Access is granted based on job role and is monitored and recorded 24/7

Access to Epic and Other Information Systems

Can I access my family, friend or co-worker's medical record?

Can I access my own medical record?

Is EHR access monitored?

Can I be terminated for inappropriate access, use or disclosure of PHI?



Privacy violations may result in disciplinary action up to and including termination of employment and could result in fines civil and/or criminal penalties against the individual workforce member.

Access is granted based on job role and is monitored and recorded 24/7

Law Enforcement and Government Oversight Agencies

When Law Enforcement Requests Patient Information

It is important that workforce members *immediately notify their supervisor, a department/unit core leader, or Admin on Call (AOC)* if approached by law enforcement so that the agent's request can be handled appropriately through our organization's procedure, no matter if they have a subpoena or a warrant for medical records.

- Requests can come through an agent, or a written document
- Always be polite to the agent

Disclosure of a patient's personal or medical information to law enforcement or government agents must be handled by Health Information Management or the designated operations area.

In some cases, the disclosure of patient information to a third party must be accounted for and documented so it is important that only designated areas familiar with these policies release patient information.

It is important to note that Providence will always cooperate with requests from government agencies, our responses will be clear and truthful, and no alteration or destruction of records will occur.

Remember: if you are not specifically trained in Government requests, you should lead the official to a supervisor.

Personal Devices

Do not text PHI

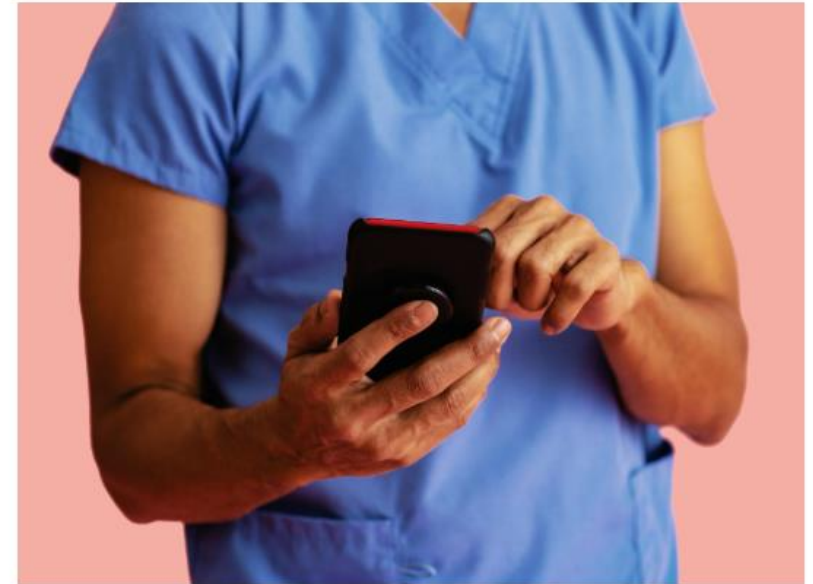
- Utilize approved communication methods (Teams, Outlook, Epic InBasket).
- If you must text in an emergency situation, text to request a phone call back or keep it generic and do not use identifiers.
- Centers for Medicare and Medicaid Services (CMS) does not permit the texting of orders by physicians or other health care providers.

If you receive confidential information on your personal device, report it but do not share it.

Never use personal mobile devices or any other personal electronic devices to capture pictures and/or videos of patients or PHI for any reason.

- A caregiver using a personal device in a patient care area or where patients are present to capture images that seemingly do not identify a patient is still a violation of policy.

Physicians may use specific apps that are integrated securely with their personal devices that allow them to upload images used for treatment to the patient's medical record.



If you see anyone violating any of these requirements report it immediately!

PHI and Social Media

1. Never post descriptions of anything related to the care or treatment of a patient, including photos and videos given to you by others, on your personal social media account. A unique story or photo that you think is de-identified may be identifiable to a patient or their family. Any disclosure of patient information on social media requires prior written authorization by the patient and approval by Marketing and Communications (MarCom). Verbal permission from the patient is not sufficient.
2. Never share confidential or proprietary information about patients, Providence or other caregivers on a private or public social media account.
3. If you identify yourself on your personal social media account as a workforce member at Providence you should make it clear that your statements and opinions are yours and are not being made on behalf of Providence.



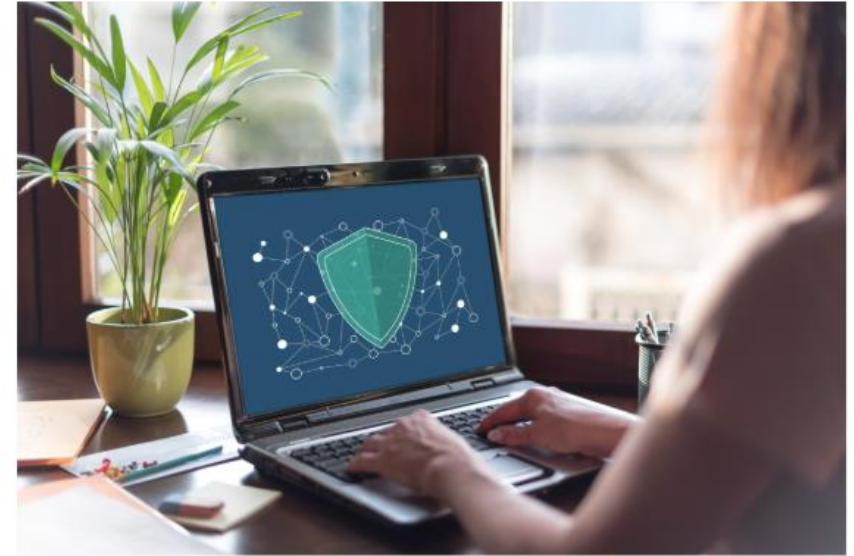
Immediately report violations of the Social Media policy to the Compliance Hotline, to your local Compliance Representative or local Caregiver Relations representative. You may ask questions as well if you do not understand this policy.

Privacy and Patient Rights Safeguards: What Should You Do?

- Understand and follow patient verification procedures that apply to your role (i.e.; use of 3 unique identifiers for registration). Many patients share full names and dates of birth and registration errors can cause significant billing issues for patients along with privacy risks.
- Understand and follow verification procedures when scanning paper documents into electronic medical records. Scanning documentation into the wrong patient's record creates not only a safety risk but can create a privacy risk if the patient accesses and views another patient's PHI.
- Be cautious with verbal conversations whether in treatment areas or in public areas. Know the audience listening.
- Keep PHI secure and out of public view (paper records, computer screens, medication with patient stickers, etc.).
- Always use a fax coversheet with contact information when sending PHI and/or confidential information.

Privacy: Key Takeaways

1. Keeping our patients' health information private is part of my role and responsibility!
2. I should be aware of privacy laws, no matter my role/job.
3. I need to understand the guidelines when sharing on social media regarding my work with Providence.
4. Access to patient's health information is only appropriate when I am part of that patient's care team, and it is against policy to access my own record.
5. I may never use a personal device to record or take pictures in patient care areas or where patients are present.
6. I cannot be subject to retaliation for reporting actual or perceived violations of policy when reporting in good faith.
7. I know how to contact my local Compliance and Caregiver Relations representatives.



Cybersecurity Overview

Taking care of patients includes securing their data and the devices used to deliver their care. By protecting patients' data, we help ensure Providence maintains their trust while providing high-quality care.

The **Cybersecurity** (CYBR) division provides information security policies along with governance, risk and compliance of important information security controls.

“

“We can put world class tools in place and hire the best (and we do!) but securing our environment requires help from everyone. We like to think of cybersecurity as a team sport.”

Adam Zoller
SVP Chief Information Security Officer

”

Cybersecurity and Acceptable Use

It is important for all workforce members to know how to appropriately use organization-owned devices and personal devices when accessing work-related systems and/or programs.

- Providence monitors the use of all information systems, all access to electronic data, and all devices that are used to access our systems or data.
- Workforce members should have no expectation of privacy with regards to content or use of Providence systems. This includes Internet usage, communications and/or transactions made that are of a personal nature while on our networks or devices.
- Only use approved Providence licensed applications, programs, and apps to conduct Providence business
 - ⊖ Never use Non-Providence licensed software, this includes free online applications as well as cloud storage.
- The use of personal email accounts are prohibited! Only use your Providence provided email account for conducting any Providence business.

All workforce members are obligated to cooperate with internal investigations or remediation efforts related to information security incidents.

Cybersecurity Best Practices

1. Keep all work passwords private and secure and do not share with anyone, ever!
 - Providence will NEVER ask you for your password, even if you are trying to reset it.
 - Use strong passphrases (at least 16 characters with a variety of characters including upper and lowercase letters, numbers, and symbols).
2. Enable multi-factor authentication.
3. Keep your devices, software and apps updated.
4. Lock or log off your computer when you walk away.
5. Use *#secure#* in your subject line when sending confidential information outside of the organization.
 - Do not send confidential information to a personal (non-business) email address.
6. A vehicle is not considered a secure location and should not be used to store confidential information, mobile computing or storage devices.
7. Always use shredder bins to dispose of confidential information.
8. To avoid phishing schemes, do not click on suspicious links or download attachments from unfamiliar senders, especially from external email addresses.
 - Use the "Report a Phish!" button in your Outlook ribbon for any suspicious emails.

Physical Security

Physical security is everyone's responsibility. The following are actions that you can take to help ensure Providence ministries/facilities are secure and our workforce members and patients are safe:

1. Always wear your badge on Providence property.
 - It is OK to inquire in a friendly and professional manner when someone is not complying with this requirement.
2. Prevent unauthorized individuals from entering confidential areas within the ministry/facility.
 - Workforce members are encouraged to inquire in a friendly and professional manner if someone does not look familiar and to validate their authorization to enter the building.
3. Do not loan out your keys or access cards; if they are lost or stolen, report it immediately to your local security personnel office.
4. Seek de-escalation training opportunities.



If you see something, say something. If you observe something that does not look, feel, or seem right, it probably isn't! REPORT IT to your local physical security department

Cybersecurity: Key Takeaways



1. Information security is part of my role and responsibility!
 - Be #CyberSmart and help defend against hackers:
 - ✓ Use strong passphrases and password managers
 - ✓ Enable multi-factor authentication
 - ✓ Keep your devices, software and apps updated
 - ✓ Don't fall for phishing attempts
2. Before downloading any program, software, and/or app to my work device, I must get approval from IS.
3. No one should be accessing my devices that contain Providence work-related information.
4. My Providence owned devices can be monitored and/or reviewed at any time. I have no expectation of privacy on these devices.
5. I know how to contact my IS team when I need them.



Quality and Patient Safety

Providence Health is fully committed to the highest standards of patient care and safety. Each of us plays an important role in achieving and maintaining these standards.

This section will provide you with information and tools to actively participate in our continuous pursuit of the best possible outcomes and no preventable harm.



Our Quality & Patient Safety Program

- Our program is dedicated to improving the quality and safety of patient care throughout Providence.
- The program focuses on continuous monitoring and evaluation of clinical practices and patient outcomes to identify areas of improvement and ensure compliance with professionally recognized standards of care and patient safety. By identifying and addressing areas for improvement, we help maintain our commitment to excellence in patient care.
- The program is led by the Chief Quality Officer for Providence's CIA-covered ministries.



Russell Shear, CIA Chief Quality Officer

The Quality Assurance and Performance Improvement (QAPI) Program

The QAPI programs of each ministry serve as foundational components of the Quality & Patient Safety Program, driving continuous improvements in patient care and safety throughout Providence.

Quality Assurance (QA): Monitors and evaluates healthcare services to ensure compliance and uphold standards, identifying areas for improvement.

Performance Improvement (PI): Uses findings from QA to initiate targeted process improvements.

The image shows the cover page of a document titled "QUALITY ASSURANCE & PERFORMANCE IMPROVEMENT (QAPI) AND PATIENT SAFETY PLAN". The page features the Providence logo at the top left. A large blue rectangular area with a geometric pattern is in the center, with the text "Put your ministry name here." below it. Below this, the title "QUALITY ASSURANCE & PERFORMANCE IMPROVEMENT (QAPI) AND PATIENT SAFETY PLAN" is displayed. A "Date" field is located below the title. At the bottom, there are three logos: "STRENGTHEN THE CORE" (orange), "BE OUR COMMUNITIES' HEALTH PARTNER" (blue), and "TRANSFORM OUR FUTURE" (green). To the right of the main content area is a table of contents.

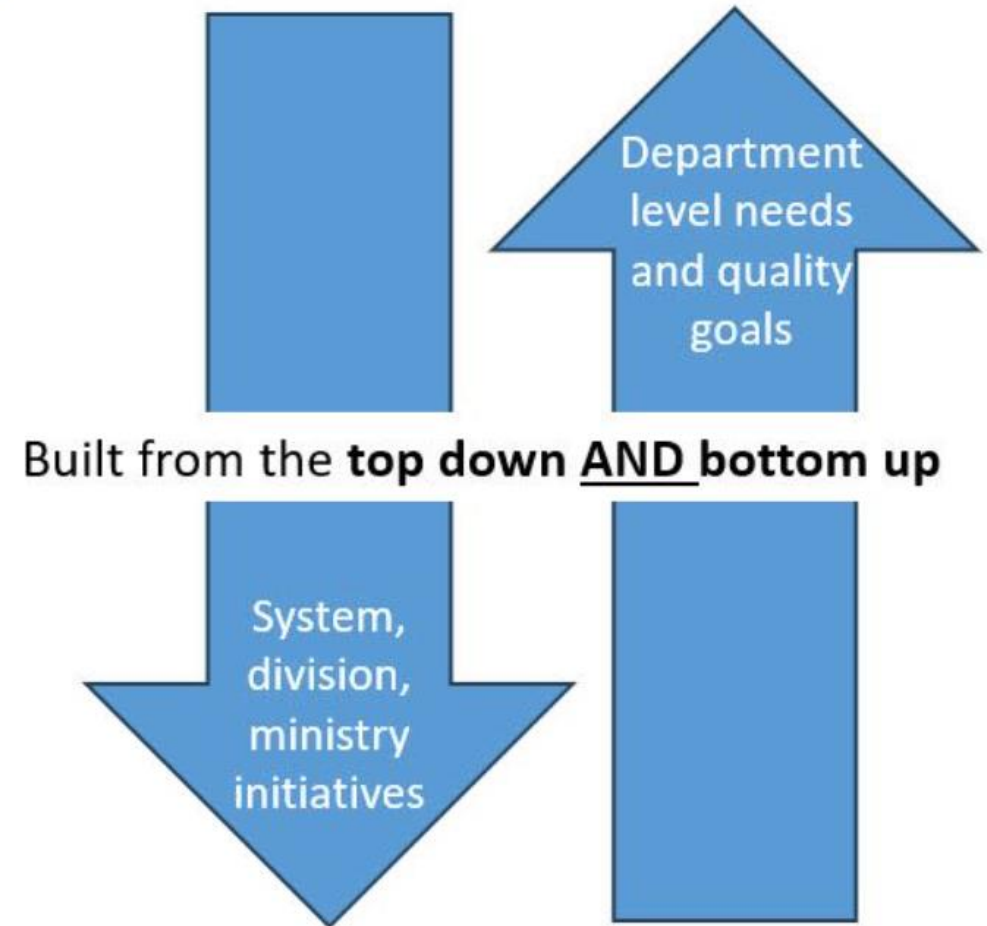
| Plan 2023-2028 | |
|----------------|---------|
| | Page(s) |
| | 3-4 |
| | 4 |
| | 4-5 |
| | 5 |
| | 5-8 |
| | 8-9 |
| | 10-12 |
| | 12-14 |
| | 15-16 |
| | 17-20 |
| | 21 |
| | 22-27 |

| |
|---|
| Appendix A: Ministry Specific Addendums |
| • Oversight and Reporting Structure |
| Appendix B: Annual Patient Safety Plan |

The Quality Assurance and Performance Improvement (QAPI) Program

A strong Quality Assurance and Performance Improvement program does the following:

1. Enables improvement in evidence-based indicators that will improve health outcomes and reduce errors.
2. Incorporates quality indicator data.
3. Prioritizes performance improvement activities that focus on high-risk, high-volume, problem-prone areas.
4. Conducts performance improvement projects that reflect the scope and complexity of the hospital's services and operations.
5. Requires ownership by executives and oversight by the ministry's governing body.



Two Important Methods for Improving Quality & Patient Safety

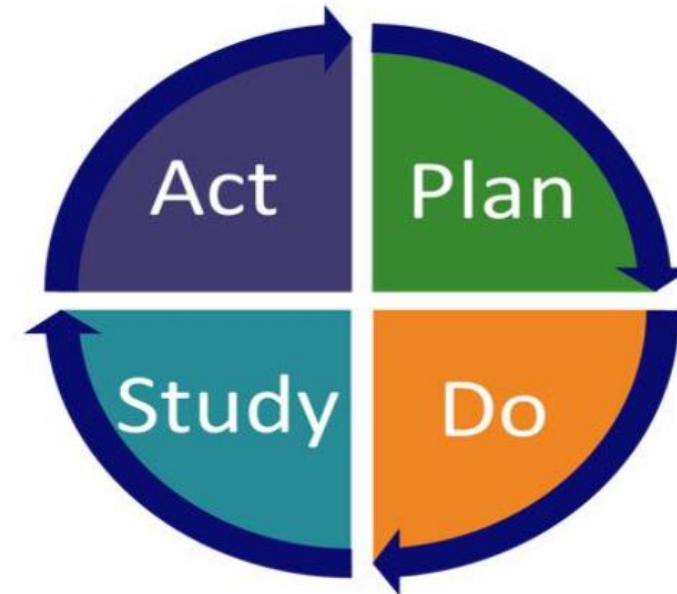
We use these improvement cycles to reinforce continuous learning and improvement in both quality – creating the best possible outcomes, and safety – ensuring no preventable harm to patient, caregivers, or our business operations.

Safety:
No preventable harm



Providence **Safety** Improvement Cycle

Quality:
Best possible outcomes



Plan, Do, Study, Act (PDSA) **Quality**
Improvement Cycle

Speak up for Safety: Quality & Safety Event Reporting

We can reduce harm to our patients and caregivers by knowing about potential and actual harm events. It is a part of everyone's job to timely report quality and safety events and concerns. This allows us to timely develop and implement appropriate actions in response to identified issues, with the goal of preventing recurrence through changes to systems and processes.

Providence seeks to create an environment where all caregivers feel empowered to speak up when they have questions or concerns.

- Retaliation against any individual who reports a quality or safety event or concern is strictly prohibited and subject to disciplinary action.
- As a High Reliability Organization, we are committed to fostering a culture of safety where fairness and just accountability are foundational principles. We recognize honest mistakes can occur and are an opportunity for learning and improvement. By embracing a just culture, we focus on understanding and correcting systems and processes, rather than on individual blame.



Speak up for Safety: Quality & Safety Event Reporting

Timely reports (as soon as possible) are used to help us identify issues so we can:

- Improve safety
- Reach out early and communicate to patients/families when events occur
- Provide support to our caregivers/providers as soon as possible when they are involved in events
- Meet regulatory requirements to report certain types of events promptly

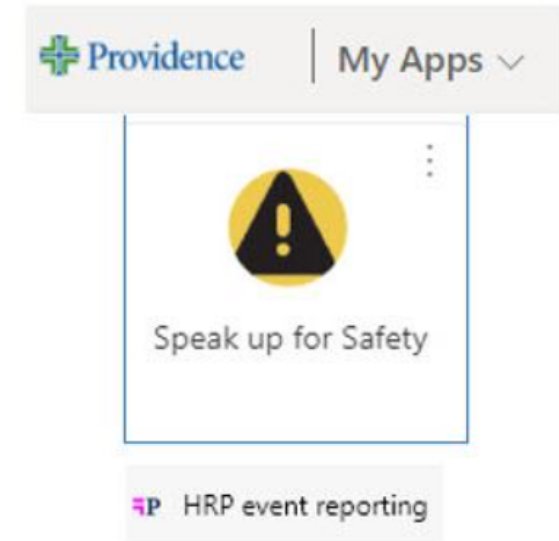
Timely reports lead to timely fact finding so we can share lessons learned with other units, departments, clinics across all of Providence, thus improving care everywhere.

High Reliability Organizations aim to have very few anonymous reports. Non-anonymous reports typically allow for more effective follow up. When the reporter is known, the Quality & Safety team can contact them directly for additional information or clarification. This can provide us with a better understanding of the issue, improve our response to the issue, and speed up the resolution process.



Speak up for Safety: Quality & Safety Event Reporting

- Report all care events that need follow-up action. These include – but are not limited to – actual harm events and hazards or defects in systems, processes, and equipment.
- Report any care event that is a good opportunity for improvement. These include – but are not limited to – defects, near miss events, and hazards.
- **Event reporting is always a good thing. When in doubt, fill it out!**
- Report medical staff concerns. These can include concerns about any aspect of care and behavior.
- Provide enough factual information in your report so your leader and quality/patient safety/risk team can have a picture of what happened. Include your contact information.
- High Reliability Platform (HRP) training is available in HealthStream. Look for the course **PROV: Submitting HRP Events**.
- HRP can be accessed via the desktop icon on your workstation or through My Apps portal.



Event Reporting Made Easy

1  Speak up for Safety (HRP)

2


Patient Safety

Workforce Safety

Service Feedback

Choose your location from the dropdowns

Add New Entry

3  Locations


☐ Report Anonymously

Create Cancel


4

Create and Complete Form


Initial Report

What day did the event occur? 


MM/DD/YYYY

What time did the event occur? 


(optional)

What day did you enter the initial report? 


03/20/2024


Please choose the type of safety event you are reporting. 


☒ Incident - event that reached the patient ☐ Near miss - event that did not reach the patient ☐ Unsafe condition


Initial impression of extent of harm at time of event 


☐ Significant injury or death ☐ Temporary or minor/moderate injury ☐ No evident harm

Select the primary location where this event occurred. 

 Locations PROVIDENCE HEALTH SYS IN ALASKA / PAMC TELEHEALTH NURSING

Select additional locations involved in the event. 

 Locations

Which category best describes the type of event or unsafe condition? 

☐ Blood or Blood Product

☐ Care Coordination / Patient Code / EMTALA

☐ Consent

☐ Device or Medical/Surgical Supply, including Health Information Technology (HIT)

☐ Diagnosis Related

☐ Environment

☐ Fall


☐ Healthcare-associated infection

☐ Infection Related

☐ IV and Line Related

☐ Medication or Other Substance (e.g., vaccines, medical gases, breast milk, enteral nutrition product)

☐ Nutrition

Type of person affected 

☒ Patient ☐ Not a Patient

Patient Details

Search to identify the patient related to this event


Encounter Id

Date

MRN


Address

If patient is not found in lookup, please enter patient first name, last name, a (optional)


Was a Caregiver involved? 

(optional)

☐ Yes ☐ No

Were any of these applicable to the event? 


None of these are applicable

Describe the event in your own words (enter facts not opinions): 

Share FACTS (not opinions) about what happened

5

Save and close



Save

Save and Close

Other Ways to Share Quality & Safety Concerns

While the Quality & Safety Event Reporting System (HRP) is the most reliable way to document an issue, quality and safety concerns can also be shared in the following ways:

- Your core leader
- During department huddles
- Higher-level manager
- A member of your local quality & safety team
- During department tracers and mock surveys

Compliance department

- If you are not comfortable using these resources or if a concern was previously reported using one of these resources and you do not believe it has been given sufficient attention, please contact the Compliance Department.
- If you have a compliance or integrity related concern, please report it to the Compliance Department.
- You can report issues or concerns to the Compliance Department via the Integrity Hotline or to a compliance staff member.

Remember: Providence strictly prohibits any form of retaliation against those who report safety events or concerns in good faith.



EMTALA

EMTALA

Select each button below for more information about the Emergency Medical Treatment and Labor Act.

What is EMTALA?

What are the main requirements of EMTALA?

When are EMTALA obligations triggered?

What constitutes an appropriate Medical Screening Exam (MSE)?

What constitutes an "Emergency Medical Condition" (EMC)?

- EMTALA stands for the "Emergency Medical Treatment and Labor Act".
- It is commonly referred to as the "patient-dumping" or "anti-dumping" law.
- Its goal is to ensure everyone has access to emergency medical services regardless of their ability to pay, insurance status, national origin, race, creed, color, age, disability, sex, or gender identity.
- It applies to all Medicare participating hospitals.
- Violations of EMTALA can result in significant fines and penalties for hospitals and physicians.

EMTALA

Select each button below for more information about the Emergency Medical Treatment and Labor Act.

What is EMTALA?

What are the main requirements of EMTALA?

When are EMTALA obligations triggered?

What constitutes an appropriate Medical Screening Exam (MSE)?

What constitutes an "Emergency Medical Condition" (EMC)?

EMTALA has three main requirements:

Conduct Medical Screening Examinations (MSE)

- Any individual who comes to the Emergency Department and requests examination or treatment must receive an appropriate MSE to determine whether an Emergency Medical Condition (EMC) exists.

Treatment to Stabilize or Appropriate Transfer

- If an EMC exists, the hospital must provide further examination and treatment to stabilize the condition or carry out an appropriate transfer to another hospital with specialized capabilities to treat the condition.

Accept Appropriate Transfers

- Hospitals with specialized capabilities are required to accept transfer from hospitals that lack the capability or capability to treat the patient.

EMTALA

Select each button below for more information about the Emergency Medical Treatment and Labor Act.

What is EMTALA?

What are the main requirements of EMTALA?

When are EMTALA obligations triggered?

What constitutes an appropriate Medical Screening Exam (MSE)?

What constitutes an "Emergency Medical Condition" (EMC)?

EMTALA is triggered when an individual **comes to** a dedicated emergency department (ED) and **requests** emergency care.

An individual **come to** the ED when he/she:

- Presents to ED,
- Is outside ED but on hospital property (entire main hospital campus, including parking lot, sidewalk, and driveway, and any building owned by the hospital within 250 yards of the hospital),
- Presents to an off-campus facility with an ED, or
- Is in a ground or air ambulance for purposes of the examination and treatment at the hospital's ED, and the ambulance is either:
 - *Owned and operated by the hospital*, even if the ambulance is not on hospital property, or
 - Neither owned or operated by the hospital, but *on hospital property*
- A **request** is made for examination or treatment when:
 - Made by the individual,
 - Made on the individual's behalf (e.g., family member, EMS personnel, etc.). Or
 - The appearance or behavior of the individual would cause a prudent layperson observer to believe the individual needed such examination or treatment.

EMTALA

Select each button below for more information about the Emergency Medical Treatment and Labor Act.

What is EMTALA?

What are the main requirements of EMTALA?

When are EMTALA obligations triggered?

What constitutes an appropriate Medical Screening Exam (MSE)?

What constitutes an "Emergency Medical Condition" (EMC)?

The goal of an MSE is to reasonably determine whether an individual has an Emergency Medical Condition (EMC), or a pregnant woman is in labor.

- Triage is not equivalent to an MSE.
- The MSE is individually tailored to presenting signs, symptoms, and medical history of the patient, as well as the capability of the hospital.
- On-call physicians, if needed, are part of the MSE process.
- Screening protocols must be applied uniformly to all patients presenting with similar symptoms.
- MSE is ongoing process with continued monitoring until it is determined whether an EMC exists, and if an EMC exists, until the individual is stabilized or appropriately admitted or transferred.
- The MSE may only be performed by Qualified Medical Personnel (QMP). QMPs are individuals determined qualified under medical staff bylaws or rules approved by the hospital's governing body.

EMTALA

Select each button below for more information about the Emergency Medical Treatment and Labor Act.

What is EMTALA?

What are the main requirements of EMTALA?

When are EMTALA obligations triggered?

What constitutes an appropriate Medical Screening Exam (MSE)?

What constitutes an “Emergency Medical Condition” (EMC)?

EMTALA defines an Emergency Medical Condition (EMC) as:

- A medical condition manifesting itself by acute symptoms of sufficient severity (including severe pain) such that the absence of immediate medical attention could reasonably be expected to result in:
 - Placing the health of the individual (or unborn child) in serious jeopardy
 - Serious impairment to bodily functions
 - Serious dysfunction of any bodily organ or part
- A pregnant woman experience contractions (unless physician or QMP acting within scope of practice certifies, after reasonable time of observation, the woman is in false labor).


An EMC can include psychiatric disturbances, symptoms of substance abuse, and intoxication. If an EMC is found *not* to exist, EMTALA obligations end.

If an EMC is found to exist, the hospital must either:

- Provide further examination and treatment to stabilize the medical condition, or
- Appropriately transfer the patient to another facility that has the capability to stabilize the medical condition.

Disclosure Program

Introduction



Providence's **Disclosure Program** seeks to foster an environment of transparency and accountability across all levels of the organization by empowering each of us to speak up when we have a question or concern. The Disclosure Program provides caregivers with a structured process for reporting concerns about actions, incidents, and practices that may be inconsistent with our Code of Conduct or the laws, regulations, professional standards of practice, and ethical commitments governing our ministry.

This program is a critical part of our compliance framework, facilitating proactive engagement from all caregivers to address potential issues early and manage risks before they become problems. It ensures all caregivers can voice their questions and concerns without fear of any form of retaliation, supporting an open dialogue essential for continuous improvement in patient care and operational integrity.

Duty to Report

As caregivers of Providence, we all share the benefit and responsibility of ensuring we honor our values and follow our Code of Conduct and policies. This includes speaking up when we have concerns.

All Providence caregivers have the responsibility to report concerns when compliance, quality of care, patient safety, or integrity are in question. This duty includes reporting potential concerns related to non-compliance with our Code of Conduct, our policies and procedures, applicable laws and regulations, and professional standards, including, among other things, items or services furnished to patients believed to have caused patient harm or to be of a quality that failed to meet professionally recognized standards of care.

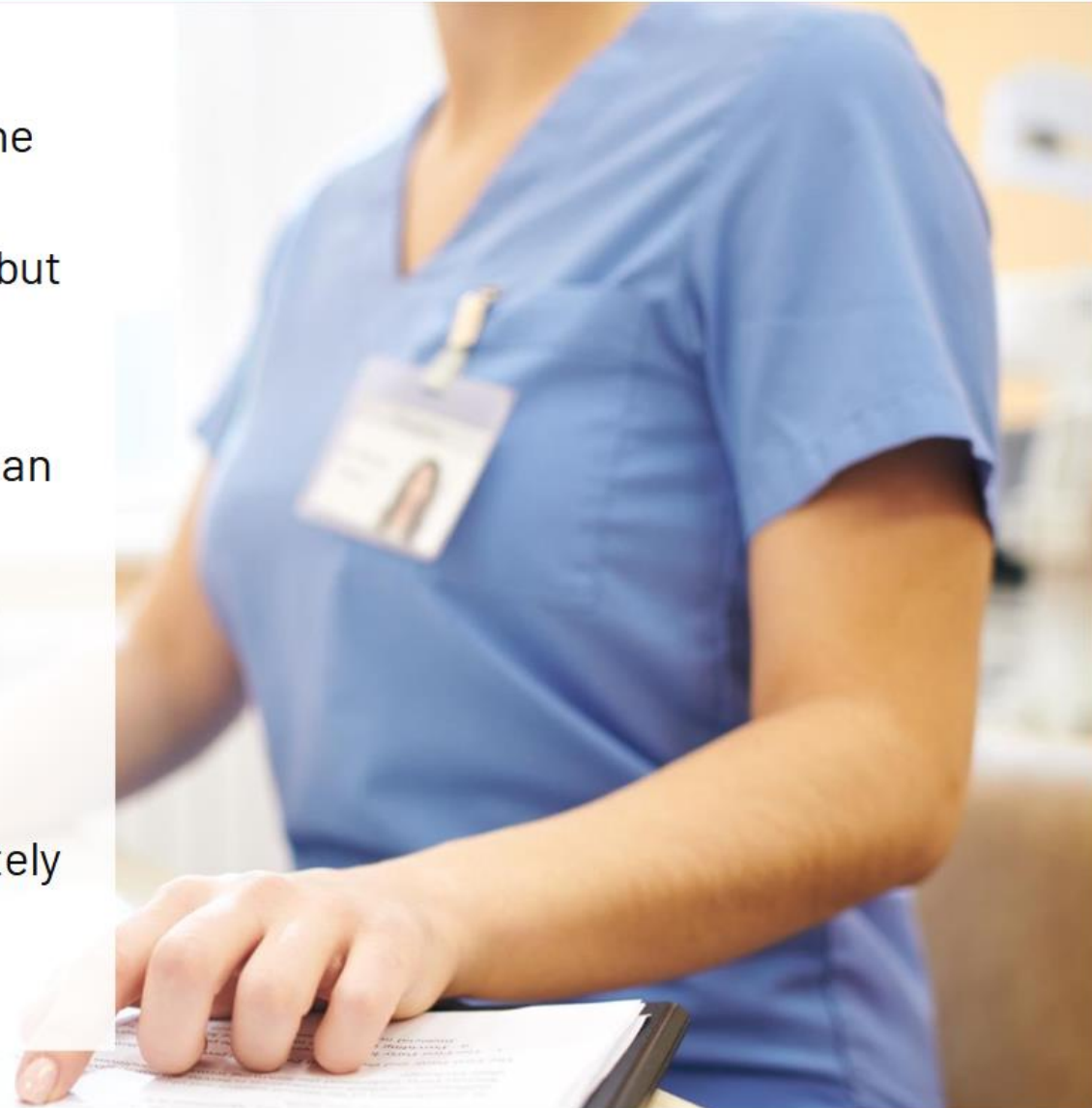
Caregivers are required to immediately report such concerns using the disclosure resources discussed in this training.

Immediate and transparent reporting of such concerns is vital to prompt resolution and preventing recurrence, helping us uphold the highest standards of compliance and patient care.

Confidentiality and Non-Retaliation

Providence is committed to maintaining confidentiality to the fullest extent possible during the disclosure process. This approach not only protects the identities of those reporting but also preserves the integrity of the disclosure process.

We encourage a fearless environment where all caregivers can report issues without the concern of retaliation. Retaliation against any individual who reports a concern in good faith is prohibited and subject to disciplinary action. Forms of retaliation could include, but are not limited to, negative performance evaluations, harassment, demotion, or unjust termination. Any such retaliatory action should be immediately reported using the appropriate resources outlined in this training.



Providence's Non-Retaliation Policy

If you are asked to do something or participate in an action that violates a Providence policy, it is your responsibility to speak up and say "no" and explain that the action seems to be a violation of policy. This applies to situations involving persons in positions of authority.

If you feel that you cannot speak up, you should immediately contact your supervisor or your supervisor's one-up, or immediately report the situation to the Integrity Hotline (which you can do anonymously) or to your local Caregiver Relations representative.

In accordance with Providence's [non-retaliation policy](#), you cannot be subject to retaliation for reporting actual or perceived violations of policy.