Status Active PolicySat ID 18219296

Origination	5/21/2025	Owner	Julie Hilsenbeck: AVP Nursing Operations
Last Approved	5/21/2025	Policy Area	Clinical
Effective	5/21/2025	Applicability	SOUTH Hospitals
Last Revised	5/21/2025		
Next Review	5/20/2030		

Providence
St. Joseph Hospital

PSJH-CLIN-1215 Falls Management Prevention

Executive Sponsor:	Darryl Elmouchi, MD, Chief Operating Officer
Policy Owner:	Julie Hilsenbeck, AVP Nursing Operations
Contact Person:	Julie Hilsenbeck, AVP Nursing Operations

THIS POLICY IS EFFECTIVE JUNE 6TH, 2025

SCOPE:

This policy applies to the not-for-profit, non-profit entities of Providence and its Affiliates [i] (collectively known as "Providence") and their workforce members (caregivers, volunteers, trainees, interns, apprentices, students), independent contractors, vendors and all other individuals working at the ministry, whether they are paid by or under the direct control of the facility; employees of affiliated organizations (collectively, "workforce members"). Where an organization is not wholly or majority owned, exceptions may apply.

This policy applies to falls management in the acute care setting.

Is this policy applicable to Providence Global Center (PGC) caregivers? ☐ Yes ☑ No

This is a management level policy reviewed and recommended by the Policy Advisory Committee for approval by senior leadership which includes vetting by Executive Leadership Committee with final approval by the President, Chief Executive Officer or appropriate delegate.

PURPOSE:

The purpose of this policy is to establish framework and guidelines for screening patient risk for falls utilizing valid and reliable tools assessing patient for specific falls risk factors, interviewing for patient history, implementing interventions for mitigating the risk for falls, actions in the event of a fall and post-fall assessment and documentation. Additionally establish guidelines for caregivers to always retain responsibility even if family is present.

The screening, assessment and recommended interventions are designed to prevent and/or reduce the number and severity of falls in the classification of anticipated physiological falls. The goal of the initiative is prevention of injury.

DEFINITIONS:

1. **Accidental Fall:** Fall that occurs unintentionally. Patients at risk for these falls cannot be identified prior to a fall and do not score at risk for falling on a predictive instrument. Environmental risks contribute to this type of fall.
2. **Unanticipated Physiological Fall:** Fall that occurs when the physical cause of the fall is not reflected in the patient's assessed risk factors for falls. These falls are created by conditions that cannot be predicted before their first occurrence (example: seizure, stroke).
3. **Anticipated Physiological Fall:** Fall that occurs in patients whose risk factor score indicated the patient is at risk of falling. Controlled sliding down a wall to the ground or utilization of a physiological structure is considered a fall. These falls are related to existing and previous risk factors.
4. **Suspected Intentional Fall:** An intentional fall event when a patient aged 5 years or older falls intentionally or falsely claims to have fallen.
5. **Developmental Fall:** A fall in which an infant, toddler, or preschooler who is learning to stand, walk, run, or pivot falls as part of the developmental process of acquiring these skills. Only falls that occur as normal parts of this learning process are developmental falls. Developmental falls should be reported only when they result in injury.
6. **Assisted Fall:** A fall in which a patient is assisted or lowered to the ground.

POLICY:

1. **SCREENING AND ASSESSMENT:**
    a. Falls Risk Screening Assessment: Nurse completes and documents age-appropriate fall scale risk screening tool during initial assessment, once per shift, upon return to inpatient unit from procedures requiring medications associated with fall risk, change in primary nurse assignment or level of care and as warranted with changes in patient condition.

    For ages 18 and above, complete a Morse Falls Risk Screening. For ages 12 months to 17 years of age, complete the GRAF-PIF General Risk Assessment for Pediatric Inpatient Falls Worksheet (GRAF-PIF Attachment A).

    b. Universal Fall Prevention Plan of Care Strategies for all Adult Patients:
        i. Following patient screening and nursing assessment for falls risk, prevention strategies customized to the patient's needs will be planned, implemented and documented. General risk reduction strategies for fall risk patients may include, but are not limited to:

1. If patient has history of falls elicit details of fall to establish any patterns. Determining if the patient was taking any risks or not following instructions will guide deeper assessment.
2. Initiate a fall risk care plan to define the patient's treatment, provide consistency of care, customize care interventions, and assess effectiveness of interventions.
3. Discuss plan of care with patient and family.
4. Offer non-skid footwear to low risk patients, apply non-skid footwear to moderate and high-risk patients.
5. Periodic reorientation if patient able to understand and retain instructions.
6. Teach the patient fall reduction actions utilizing the Falls Prevention – Patient and Family Education (Attachment B) and teach back methodology.
7. Educate patient and family to call for assistance for ambulation, toileting, transfer, and reinforce as needed.
8. Place Fall Prevention Escalation Guide signage in patient room (Attachment C).
9. Keep bed in lowest position and brakes locked, unless appropriate for care (i.e., transfer, turning patient).
10. Clear the walking area.
11. Turn on lights if needed. Maintain sufficient lighting.
12. Place call light and needed items close to patient and validate patient understanding of call light use through teach back.
13. Assess patient for 4 P's [position, pain, potty, and proximity of personal items to eliminate confusion or frustration].
14. Keep assistive devices (eyeglasses, dentures, walkers, canes) in close proximity to the patient.
15. Keep personal (phone, television remote, bedside table) and safety (call light) items near the patient.
16. Assign patients to beds that permit exiting on patient's stronger side when possible.
17. Use of less than 4 side rails or 4 rails used to protect the patient from falling out of bed, i.e. when sedated, experiencing involuntary movement, or on certain types of therapeutic beds.
18. Patients with impaired gait and balance may require referral to appropriate discipline for specific assessment, i.e., PT and may consider using lift equipment for transfer.
19. Remove wheelchair leg rests when applicable to prevent entanglement.

        20. Implementing multidisciplinary care conferences with participation of the care team.
        21. Minimize, when possible, the presence of electrical cords and unused equipment in patient areas.
        22. Provide psychological and emotional support.

c. Nurse Driven Plan of Care Strategies Based on Adult Fall Risk Score: Risk reduction strategies for fall risk patients may include, but are not limited to:
    i. Low risk for fall:
        1. Scores 0-24 on Morse scale
        2. Implement the following nurse driven interventions:
            a. Universal interventions
            b. If patient tethered consider demonstration and return demonstration for removal of oxygen tubing, telemetry leads, etc. if patient has capacity to perform.
            c. Continue to monitor and assess for any changes.

    ii. Moderate risk for fall:
        1. Scores 25-44 on Morse scale
        2. Implement the following nurse driven interventions:
            a. Universal interventions
            b. Apply**YELLOW** fall risk armband and **YELLOW** fitted non- skid socks.
            c. Have patient demonstrate use of call light. Place call light and needed items close to patient and validate patient understanding of call light use through teach back.
            d. Initiate bed and/or chair alarm to signal patient movement.
            e. Consider proactive toileting if patient experiencing urgency.
            f. If patient receiving diuretics, consider diuretic rounds one hour post medication administration.
            g. Consider teaching patient to sit up slowly and count to 60 while dangling before attempting to rise.
            h. Consider increasing frequency of purposeful rounding to anticipate and address patient needs.
            i. If patient on telemetry, treat "leads off" as alarm which may signal patient attempting to get out of bed.
            j. Consider remote visual monitoring.

iii. High risk for fall:

1. Scores 45 and above on Morse scale.
2. Implement the following nurse driven interventions:
    a. Universal interventions
    b. Apply [Insert Color] fall risk armband and fitted [Insert Color] non-skid socks.
    c. Place high fall risk sign on room door and in room within patient's view.
    d. Initiate bed and/or chair alarm to signal patient movement.
    e. Consider proactive toileting if patient experiencing urgency.
    f. If patient receiving diuretics, consider diuretic rounds one hour post medication administration.
    g. Relocate patient to a room close to nurse's station if possible.
    h. Consider leaving door open for visualization.
    i. Consider a low bed (top of mattress within 18 inches from floor) for ease of entering and exiting the bed, protection from rolling out of bed, and allows placement of feet flat on the floor while sitting on the edge of the bed.
    j. Consider using a fall mat.
    k. Have patient demonstrate use of call light. If unable to demonstrate call light, consider remote visual monitoring or constant observer.
    l. Consider increasing purposeful rounding to anticipate and address patient needs.
    m. Do not leave patient alone in bathroom or on toilet/ commode. Must stay in arm's length of patient.
    n. Caregivers must always be with patient when transferring out of bed, ambulating, or in bathroom.
    o. Utilize a gait belt when transferring or ambulating patient, excluding obstetrical patients.
    p. Consider diversional/expressive activities to engage and stimulate patient. (Examples: folding washcloths, fidget toys, stress balls, activity apron, etc.)
    q. If patient on telemetry treat "leads off" as alarm which may signal patient attempting to get out of bed.
    r. If patient impulsive, unable to re-orient or unable to

retain instructions consider Remote Visual Monitoring or Constant Observer

s. Consider the following: Can the patient be effectively reoriented? Can the patient recall simple instructions? Does the patient recognize they are in the hospital? Is the patient tethered to any equipment such as compression stockings, device or telemetry? Is the patient restless? Does the patient have urinary urgency? Has the patient had any episodes of delirium? If patient experiencing any of these implement interventions for that risk factor.

3. If above interventions have failed, consider remote visual monitoring or a constant observer

iv. Plan of care strategies and interventions for the care of adult specialty populations may be considered, see Care of Adult Specialty Populations (Attachment D).

2. **Patient/Family Education Adult**

a. Complete and review the Falls Prevention – Acute, Patient and Family Education Tool (Attachment B) with the patient/family. Ask the moderate and high-risk patient to repeat instructions back to assess for information retention.

b. Provide any additional education appropriate to the patient and his/her condition. Education subject matter may include but is not limited to:

i. Provide brochures and/or signage as reminders to use call light for caregiver assistance with transferring or ambulating.

ii. Remind family to always call caregivers for assistance with ambulation, transferring and toileting.

iii. Educate proper techniques to prevent orthostatic hypotension (i.e., changing positions slowly and avoiding prolonged sitting)

iv. Educate proper use of assistive devices such as cane or walker and have patient return demonstrate use.

v. Educate that the prescribed medications, for the current treatment plan, may increase the risk for falls during the hospital stay and upon discharge.

3. **Adult Patient Handoff**

a. The nurse provides bedside report to receiving nurse during change of shift, change in primary nurse assignment and upon patient transfer to include but not limited to the last Morse score, variables contributing to Morse score, patient's fall risk level, and interventions in place.

b. Include any cognitive deficits including disorientation, inability to retain instructions or be re-oriented and impulsivity and specialty considerations.

4. **Falls Screening and Assessment for Pediatric Patients**

a. The General Risk Assessment for Pediatric Inpatient Falls Worksheet (GRAF-PIF Attachment A) will be used for all pediatric inpatients greater than 12 months to 17 years of age. All pediatric patients will be evaluated during initial nursing assessment, once a shift, after completion of procedures requiring medications associated with fall risk, change in nurse assignment or level or care and as warranted with changes in patient condition or transfer to another unit. Change in condition may include but is not limited to postoperative, change in mental status, change in mobility, additional medical equipment, addition of medications identified as high risk for falls, any deterioration in status.

   i. Once identified to be at risk of falling, the patient remains at risk the remainder of their hospitalization and the focus moves to implementation of preventive measures.

   ii. If the GRAF-PIF score is 1 or less, implement universal fall prevention interventions for hospitalized children. If the score is 2 or greater, implement high risk fall prevention interventions.

   iii. If the child has past history of falling, either at home or during previous hospitalization, implement high risk fall prevention strategy regardless of current GRAF-PIF score.

b. Universal Fall Prevention Plan of Care Strategies for Pediatric Patients:

   i. Teach Parent/guardian or responsible adult utilizing the “Children Are at Risk of Falling While Hospitalized!” (Attachment E).

   ii. Utilize the appropriate bed type for the chronological or developmental age of the patient. If age-appropriate bed not available, caregiver must be in attendance at all times. Parent/guardian or responsible adult encouraged to stay with patient in addition to caregiver.

   iii. Orient to room and bed/crib; ensure that Parent/guardian or responsible adult knows how to operate side rails of the bed or crib.

   iv. Keep bed in lowest position and brakes locked, unless appropriate for cares (i.e., transfer, turning patient).

   v. Do not leave side of bed if rails are down.

   vi. Maintain hand contact if side of crib is down.

   vii. Keep bed wheels locked when bed is stationary.

   viii. Ensure patient has proper footwear to prevent slips if patient is mobile.

   ix. Avoid clothing that is too long and could contribute to a fall.

   x. Offer proactive toileting appropriate to developmental stage.

   xi. Use safety straps on all equipment such as swings, infant seats, wheelchairs and physical therapy devices.

   xii. Teach use of call light if developmentally appropriate.

   xiii. Place personal items within reach.

   xiv. Set behavioral limits (discourage jumping, climbing) and monitor patient and Parent/guardian or responsible adults' ability to comply. Re-educate and emphasize risk as needed.

xv. Discuss safest sleeping arrangements for patient with Parent/guardian or responsible adult.

xvi. Teach Parent/guardian or responsible adult:

1. Not to sleep in chair/couch/bed with child.
2. Be aware that as children feel better their activity level increases, and running or climbing may occur.
3. Activity limitations while hospitalized need to be continually reinforced.

xvii. Educate Parent/guardian/responsible adult that the prescribed medications, for the current treatment plan, may increase the risk for falls during the hospital stay and upon discharge.

c. Nurse Driven Plan of Care Strategies for High-Risk Pediatric Patients Based on Fall Risk Score:

i. Initiate Universal interventions fall bundle of nurse driven interventions.

ii. Apply **[Insert Color]** fall risk armband and appropriately fitted [Insert Color]

iii. non-skid socks.

iv. Place high fall risk sign on room door and in room within parent/ responsible adult's view.

v. Relocate patient to a room close to nurse's station if possible.

vi. Consider leaving door open for visualization.

vii. Consider using a fall mat.

viii. Consider increasing purposeful rounding to anticipate and address patient needs,

ix. e.g. post diuretics.

x. Caregivers will reinforce the importance of having a Parent/guardian or responsible adult or caregiver in attendance when patient is transferring out of bed, ambulating, or in the bathroom.

xi. Consider diversional/expressive activities to engage and stimulate patient.

xii. Reinforce activity limitations.

xiii. Request physical therapy consult for gait or balance issues.

xiv. Assess the need to place an age-appropriate patient in a crib with rail extensions ("bubble top") if climbing over the side rails of an adult bed.

xv. Assess the need for a Constant Observer when there is no caregiver or Parent/guardian or responsible adult in the room.

xvi. For infant drop prevention, assess the need for the use of a Remote Visual Observation or Constant Observation.

xvii. Educate parent/guardian/responsible adult on drop prevention.

5. **Hand Off Pediatric:**
   a. The nurse provides bedside report to receiving nurse during change of shift, change in primary nurse and upon patient transfer to include but not limited to the last GRAF-PIF score, variables contributing to score, patient's fall risk level, and interventions in place.

6. **Adult and Pediatric Medication Classification Assessment:**
   a. If the patient is prescribed medications from the Medication Classification List (Table A), the patient is at moderate risk for falls, if not previously identified as high risk on screening tool. Individually prescribed high risk medications and multiple prescribed medications may place the patient at risk for falls.

   b. If there is/are secondary diagnosis listed, the medication classifications related to the secondary diagnosis(es) may be a determinant of potential falls risk. Table A provides several of the highest risk medication classes that place patients at risk for falls. If the patient is prescribed medications from Table A, the patient should be considered at risk for falls.

Table A: Medication Classifications

Anti-seizure medications	**Blood Thinners***	Psychotropics
Anti-arrhythmics	Diuretics	Sedating Antihistamine
Anti-hypertensives	Laxatives	Sedative/hypnotics
Benzodiazepines	Narcotic analgesics	Skeletal muscle relaxants

*Blood thinners are included although not directly contributing to falls, may cause severe complications with a fall. Blood thinners may include but are not limited to anticoagulants, aspirin, over the counter herbal agents which may impact clotting times.

7. **Environment of Care Assessment for Risk Mitigation Considerations:**
   a. Patient care areas will be assessed at least annually by a multidisciplinary team including but not limited to Chief Nursing Officer/designee, risk manager, quality director, facilities director, unit director, direct caregivers to identify environmental factors which may contribute to patient falls. Findings will be reported to the facility quality committee.

   b. Environmental fall risk assessments should be completed periodically even if a specific unit or population has previously been assessed and determined to present minimal fall risk.

   c. When assessing environmental fall risk factors, consider the types of patients served, the services provided and the physical environment (e.g., is the population elderly, mobile, post-surgical, etc.).

   d. Environmental fall risk reduction assessment should be integrated into existing fall reduction initiatives.

   e. Environmental safety features to consider:
      i. Transfer equipment

ii. Non-slip flooring

iii. Height-adjusted bed

iv. Raised toilet seats

v. Elimination of sharp edges

vi. Use of safe exit side from bed

vii. Use of bed alarms and chair alarms, including Virtual Bed Rails

viii. Access to mobility aids such as canes, walkers, etc.

ix. Assess IV poles for easy tipping (adjust the height of the IV pole to facilitate ambulation).

x. Review environmental services policy for identifying and addressing wet floors.

8. **Post-Fall Management**:

   a. Follow the Post-Fall Response Protocol

   b. Document the fall under the Critical Incident to trigger falls related documentation in Epic (post fall assessment and 18-hour reassessment).

   c. Implement the following interventions:

      i. If the patient is unstable, vital signs are deteriorating, or neurological changes; Don't leave the patient unattended, call for a Rapid Response Team, and notify the provider.

      ii. Assess for injuries and consider the following:

         1. Those over 65 are at higher risk for c-spine injury after a ground-level fall, and, if c-spine injury is present, suspect a high-level injury (e.g., Cervical Vertebrae, C-1 or C- 2).

         2. Patients who complain of neck pain are more likely to have cervical spine injury.

         3. Patients who have a loss of consciousness after a fall are at higher risk for brain and cervical spine injury.

         4. Patients with osteoporosis or other bone diseases such as bone cancer or bone metastasis are more likely to suffer injury after falls.

         5. Patients who take anticoagulant medications (aka blood thinners) are more likely to suffer from bleeding, organ injury, and brain hematoma because of a fall.

         6. Evaluate how traumatic the fall was. A patient who is eased to the ground is less likely to sustain injury than those who fail to brace a fall. Typically, patients will try and protect themselves by holding out their arms.

   d. Obtain vital signs

      i. Immediately and then:

        1. Every hour X 4
        2. Every 4 hours X 6

e. For unwitnessed falls or witnessed falls with impact to head/neck, or change in Level of Consciousness (LOC), Perform a neurological check with attention to level of consciousness, neck pain, or deficits in the extremities. Any patients with a known or suspected head injury or intracranial bleed, notify the provider and continue neuro checks:

    i. Every hour X 4

    ii. Every 4 hours X 6

f. Assess for cervical spine injury by asking about neck pain and observing for any neuro deficits.

    i. Cervical spine stabilization is not recommended as a universal intervention for ground-level falls as there are complications associated with spinal immobilization. Spinal precautions are a set of measures taken to prevent movement of the spine in patients who may have a spinal injury.

    ii. Spinal Precautions:

        1. Cervical Collar: Use a cervical collar to immobilize the neck and prevent movement
        2. Log Roll Technique: If moving the patient is necessary, ensure that at least three caregivers are available to perform a log roll to keep the spine in alignment.

    iii. The following findings would warrant spinal precautions be implemented:

        1. Neck pain with a history of trauma
        2. Significant head, chin or facial trauma
        3. Significant multiple system trauma
        4. New numbness or weakness of any extremity
        5. Loss of consciousness
        6. New alteration of mentation
        7. Any significant distracting injury

g. Assess the patient for any other associated injuries such as:

    i. Abrasions

    ii. Contusions

    iii. Lacerations

    iv. Fractures or sprains

    v. Head injuries

    vi. Bleeding

h. Notify and document

i. Notify the patient’s provider

ii. Notify the patient’s emergency contact

iii. Notify the clinical leader on duty

iv. Complete a post-fall assessment in EHR

1. Post fall assessment documentation is performed by the primary Registered Nurse (RN). When the Rapid Response Team (RRT) is involved, they work in conjunction with the primary RN to complete documentation and care plan.

i. Document the details of the fall and interventions deployed in the patient’s medical record.

j. Submit an event report in the High Reliability Platform (HRP).

9. **Post-Fall Debrief**

a. A post fall debrief must occur during the shift the fall occurred. Include primary caregivers such as nurse, therapist, charge nurse and the patient when possible. Families are notified of a patient fall as soon as possible unless specifically directed by the patient not to notify them.

b. All questions must be answered.

c. Stay focused on what could be done to prevent and avoid placing blame

i. The purpose of the post fall debrief is to: Make immediate changes to the patient's plan of care to prevent further falls

ii. Share learnings from debrief with other caregivers caring for the patient

iii. Share collective learning to evaluate practices and processes that contributed to the patient fall

10. **Data Collection and Reporting**

a. Data will be collected and collated. These data will be graphed and reported monthly to the appropriate ministry and/or Falls Committees. This will be used for Performance Improvement and other organizational reports. Additional reports may be added at facility discretion.

11. **Associated Policies/Procedures:**

a. System Constant Observer Policy, Ministry Remote Visual Monitoring policy

SOUTH DIVISION-SPECIFIC ADDENDUM:

- Where noted in policy for (insert color), in California ministries will utilize yellow fall risk armbands and yellow fitted non-skid socks.
- Notification to the patient’s emergency contact (reference Policy Section 8.h.ii) should be done only after obtaining permission from a patient that is alert and oriented as they maintain decision making authority unless otherwise delegated to a surrogate decision maker.

RELATED POLICIES:

PSJH-CLIN-1216 Restraint for Non-Violent Non-Self-Destructive Behavior

PSJH-CLIN-1217 Restraint for Violent and Self-Destructive Behavior

PSJH-CLIN-1218 Suicide Screening

PSJH-CLIN-1219 Constant Observer

REFERENCES:

AHRQ Fall Prevention in Hospitals Toolkit (2018)

Cooper, C, Nolt, J (2007) Development of an Evidence-based Pediatric Fall Prevention Program, *Journal of Nursing Care Quality* 22(2), 107-112.

Ganz DA, et al: Preventing falls in hospitals: A toolkit for improving quality of care. Prepared by RAND Corporation, Boston University School of Public Health, and ECRI Institute.

Graf, E. (2004). *General Risk Assessment for Pediatric Inpatient Falls Scale Worksheet (GRAF-PIF).* Fall Risk Assessment Tool, Children's Memorial Medical Center.

Guirguis, J., Michael, Y., Perdue, L., Coppola E., & Beil, T (2018). Interventions to Prevent Falls in Older Adults- Updated Evidence Report and Systematic Review for the US Preventative Services Task Force.

McGreevey, M (2005, September). Examining inpatient pediatric falls: Understanding the reasons and finding the solutions, *Joint Commission Perspectives on Patient Safety*, 5(9), 5-6.

Morse, J. Enhancing the Safety of Hospitalization by Reducing Patient Falls. *American Journal of Infection Control*, Vol. 30 (6), October, 2002, pg. 376-380.

Morse JM, et al: A prospective study to identify the fall-prone patient. Social Science and Medicine, 1989:28(1)81- 6.

Morse JM, et al: Development of a scale to identify the fall-prone patient. Canadian Journal on Aging, 1989;8;366- 7.

Morse JM: Preventing patient falls. Thousand Oaks, California: Sage Publications, 1997. 20.

Oliver, D & Healy, F., (2010). Preventing falls and fall-related injuries in hospitals. Clinical Geriatric Medicine, 26, 645-692.

Oneil, C., Krauss, M., Bettale, J., Kessels, A., Costantinou, E., Dunagan, C., & Fraser, V. (2018). Medications and Patient Characteristics Associated with Falling in the Hospital. Journal of Patient Safety, 14, 1, 27-33.

Razmus, I, Wilson, D, Smith, R, Newman, E (2006) Falls in Hospitalized Children,

Pediatric Nursing 32(6), 568–572.

Sentinel Event Alert 55, (2015). Preventing falls and fall-related injuries in health care facilities A complimentary publication of The Joint Commission Issue 55.

VA National Center for Patient Safety (NCPS). (2000). *NCPS Concept Dictionary*.

Walsh, C., Liang, L., Grogam, T., Coles, C., McNair, N., et al (2018). Temporal Trends on Fall Res with the Implementation of Multi-faceted Fall Program: Persistence Pays Off. The Joint Commission Journal on Quality & Patient Safety, 44, 75-83.

APPLICABILITY:

[i] For purposes of this policy, “Affiliates” is defined as any not-for-profit or non-profit entity that is wholly owned or controlled by Providence St. Joseph Health (PSJH), Providence Health & Services, St. Joseph Health System, Western HealthConnect, Kadlec, Covenant Health Network, Grace Health System, Providence Global Center*, NorCal HealthConnect, or is a not-for-profit or non-profit entity majority owned or controlled by PSJH or its Affiliates and bears the Providence, Swedish Health Services, St. Joseph Health, Covenant Health, Grace Health System, Kadlec, or Pacific Medical Centers names (includes Medical Groups, Home and Community Care, etc.). *Policies and/or procedures may vary for our international affiliates due to regulatory differences.

Attachments

Falls Attachment A - GRAF PIF Worksheet.pdf

Falls Attachment B - Patient and Family Education.pdf

Falls Attachment C - Fall Prevention Escalation.pdf

Falls Attachment D - Care of Adult Specialty Populations.pdf

Falls Attachment E - Children - Risk Factors for.pdf

Falls Attachment F - Sample Room and or Bathroom Signs.pdf

Approval Signatures

Step Description	Approver	Date
President/CEO	Cynthia Johnston: Principal Compliance Consultant	5/21/2025
Executive Council	Cynthia Johnston: Principal Compliance Consultant	5/21/2025

Policy Advisory Committee	Cynthia Johnston: Principal Compliance Consultant	5/21/2025

Applicability

CA - Healdsburg Hospital, CA - Petaluma Valley Hospital, CA - Providence Cedars-Sinai Tarzana MC, CA - Providence Holy Cross MC, CA - Providence LCM MC San Pedro, CA - Providence LCM MC Torrance, CA - Providence Mission Hospitals, CA - Providence Queen of the Valley Medical Center, CA - Providence Redwood Memorial Hospital, CA - Providence Saint John's Health Center, CA - Providence Saint Joseph MC, Burbank, CA - Providence Santa Rosa Memorial Hospital, CA - Providence St. Joseph Hospital - Eureka, CA - Providence St. Joseph Hospital Orange, CA - Providence St. Jude Medical Center, CA - Providence St. Mary Medical Ctr Apple Valley

Standards

No standards are associated with this document

Status Active PolicyStat ID 12761546

Origination	08/2014	Owner	Jacqueline Daley: Senior Director Infection Prevention
Last Approved	12/2022		
Effective	12/2022		
Last Revised	12/2022	Policy Area	Infection Prevention
Next Review	12/2025	Applicability	CA - Divisional/ Regional
		References	South Division

To find another policy, use the browser BACK ← button to return to your Ministry.

Standard Precautions & Transmission-Based Precautions

PURPOSE

In keeping with the mission and values of Providence St. Joseph Health, the policy of Providence Health System - Southern California, in order to protect patients, caregivers, physicians, and others, guides the placement of patients in appropriate precautions when indicated. The Centers for Disease Control and Prevention's (CDC) two-tier system of precautions is followed – Standard Precautions and Transmission-Based Precautions.

Sub-Acute and Transitional Care Units will follow this policy unless other facility specific policies are in place.

POLICY

Categories of Isolation Precautions:

1. **Standard Precautions** is the primary practice used for the prevention of the spread of disease and infections. Standard Precautions are used in the care of all patients regardless of their diagnosis or presumed infection status and continues even when transmission-based precautions are implemented.
    a. Standard Precautions are based on the principle that all blood, body fluids, secretions, excretions (except sweat), non-intact skin, and mucous membranes may contain transmissible infectious agents such as Hepatitis B virus (HBV), Hepatitis C virus (HCV), Human Immunodeficiency Virus (HIV), and other bloodborne diseases and conditions.
    b. Standard Precautions are intended to reduce the risk of transmission, and/or acquiring, of microorganisms through healthcare workers and hospital environment.
    c. All caregivers including clinical and non-clinical caregivers are expected to follow appropriate precautions to prevent exposure to blood or body fluids, secretions, and

excretions.

2. **Transmission-based Precautions (i.e., Airborne, Droplet, Contact, Contact Enteric)** are to be implemented by nursing for patients with confirmed or suspected infections or diseases caused by epidemiologically important/significant pathogens that can be transmitted by airborne or droplet route, or by direct and indirect contact with the patient, contaminated surfaces, or equipment in the patient's/resident's environment.
    a. Transmission-Based Precautions are implemented to prevent and/or reduce the risks of acquiring and/or transmitting pathogens, highly contagious or virulent diseases/ infections, and other epidemiologically important/significant microorganisms to caregivers, visitors, and patients.
3. The supervisor or manager of the department/unit is responsible for their caregivers' compliance to the practice of Standard Precautions as well as assuring that appropriate personal protective equipment (PPE) supplies are available in the department/unit as needed for Isolation Precautions.
4. PPE is to be used consistently whenever any bodily substances or other potentially infectious material (OPIM) are likely to be in contact with a caregivers' hands, mucous membranes, clothing, and/or when touching mucous membranes or non-intact skin.

Definitions

- **Airborne Infection Isolation Room (AIIR):** Room that has monitored negative air pressure/air flow in relation to the surrounding areas and appropriate discharge of air outdoors or monitored high-efficiency particulate air (HEPA) filtration of room air before the air is circulated to other areas in the hospital
    - Each ministry-specific policy lists and includes the AIIR in an attachment.
- **Medical Face Mask:** Items used to cover the nose and mouth, and includes both procedure and surgical masks. The medical face masks assist in protecting the wearer from: inhaling large-particle aerosols (droplets) that are transmitted by close contact that travel only short distances of about three feet, and from inhaling small-particle aerosols (droplet nuclei) that remain suspended in the air and thus travel longer distances. The use of a medical face mask is not a replacement for a fit-tested N95 respirator in preventing diseases transmitted by the airborne route. The medical face mask prevents transmission of some infections that are spread by direct contact with mucous membranes as it presents a barrier to splash transmission is provided.
- **Respirator**
    - **Powered Air Purifying Respirator (PAPR):** Battery-powered helmet that uses a blower to force the ambient air through air-purifying filters or cartridges to the inlet covering.
    - **Controlled Air Purifying Respirator (CAPR):** Advanced respiratory protection helmet system/equipment approved by the U.S. National Institute for Occupational Safety and Hazard (NIOSH) for protection against aerosolized and airborne particulates and meets the loose-fitting PAPR requirements of CalOSHA.
    - **N95 Respirator:** A respiratory protective device designed to achieve a very close facial fit and very efficient filtration of airborne particles. Note that the edges of the respirator are designed to form a seal around the nose and mouth. Surgical N95 Respirators are commonly used in healthcare settings and are a subset of N95 Filtering Facepiece Respirators (FFRs).

- **Personal Protective Equipment:** Specialized clothing or equipment, worn by an employee for protection against infectious materials.
- **Cohorting:** In the context of this policy, applies to the practice of grouping together patients infected or colonized with the same infectious agent to confine their care to one area and prevent contact with susceptible patients (referred to as patient cohort). During outbreaks, caregivers may be assigned to a cohort of patients to further limit opportunities for transmission (referred to as caregiver cohort).
- **Epidemiologically important/significant pathogens:** Infectious agents that have one or more of the following characteristics:
    - Antimicrobial resistance implications:
        - Resistance to first-line therapies (e.g., *Carbapenem-resistant Enterobacterales* (CRE), Vancomycin-Intermediate *Staphylococcus aureus* (VISA), Vancomycin-Resistant *Staphylococcus aureus* (VRSA), *Clostridioides difficile (C. diff*), multi-drug resistant Gram negative rods).
        - Unusual or usual agents with unusual resistance patterns within a facility.
        - Difficult to treat because of innate or acquired resistance to multiple classes of antimicrobial agents.
    - Associated with serious clinical disease, increased morbidity and mortality.
    - A newly emerging or re-emerging pathogen.
- **Multi-Drug Resistant Organism (MDRO):** Difficult to treat because of innate or acquired resistance to multiple classes of antimicrobial agents.
- **Endemic Organism:** Infectious agent commonly found in the community population or region that is not epidemiologically important/significant (e.g., Methicillin-resistant *Staphylococcus aureus* (MRSA), Vancomycin-resistant Enterococcus (VRE), Extended-spectrum Beta lactamase (ESBL) organisms.
- **Biohazard Waste:** Waste that has the risk of carrying infectious diseases; includes blood and all other potentially infectious materials (e.g., dressings soaked, dripping, or bloody).

Equipment

Personal Protective Equipment (PPE):

1. PAPR/CAPR
2. Disposable non-sterile gloves (non-latex and nitrile)
3. Medical face mask
4. N95 Respirator
5. Eye protection (goggle/face shield)
6. Gown with 360-degree coverage
7. Supplemental equipment:
    a. Biohazardous waste disposal bags
    b. Clear plastic bags
    c. Biohazardous specimen bags

d. Sharps containers

e. Disposable assessment, monitoring, and/or resuscitation devices

Standard Precautions

PROCEDURE/GENERAL INSTRUCTIONS

Assume that every patient is potentially colonized or infected with an organism that could be transmitted in the healthcare setting. Applies to any of the following infection prevention practices/interactions during the delivery of patient care.

Infection Prevention Practices

1. **Hand Hygiene** *(Refer to* PSJH-CLIN-1205 Hand Hygiene Policy f*or further details)*.

    a. Only hospital-approved alcohol-based hand rub or soap and water are acceptable for hand hygiene.

    b. Indications for hand hygiene include but are not limited to:

        i. Before having direct contact with patients.

        ii. Before donning sterile gloves when inserting a central intravascular catheter.

        iii. Before inserting indwelling urinary catheters, peripheral vascular catheters, or other invasive devices that do not require a surgical procedure.

        iv. After contact with a patient's intact skin (e.g., when taking a pulse or blood pressure, lifting a patient).

        v. After contact with body fluids or excretions, secretions, mucous membranes, non-intact skin, and wound dressings. If hands are visibly soiled, perform hand hygiene with soap and water.

        vi. If moving from a contaminated body site to a clean body site during patient care.

        vii. After contact with inanimate objects (including medical equipment) in the immediate vicinity of the patient.

        viii. Before donning exam gloves and after removing exam gloves.

        ix. Before administering medication.

        x. Before accessing invasive devices.

        xi. After covering a cough or sneeze.

        xii. After using the bathroom – use soap and water.

        xiii. At any time it is felt that hands may be contaminated

2. **Personal Protective Equipment (PPE)** which includes the use of any or all of the following: gloves, gown, mask, face shield, shoe covers, head covers, respirators, etc., when contact with blood or body fluids or other communicable toxins or agents is anticipated. PPE must be removed before exiting the patient's room and hand hygiene performed.

    a. *Review Donning and Doffing Personal Protective Equipment (PPE) Policy (***PolicyStat ID:** *9790601) and/or CDC donning and doffing sequence (*https://www.cdc.gov/hai/pdfs/ppe/ppe-sequence.pdf).

b. *Gloves*

   i. Perform hand hygiene before donning and after removing gloves.

   ii. Wear gloves when it can be reasonably anticipated that contact with blood or other potentially infectious materials, mucous membranes, non-intact skin, or potentially contaminated intact skin (e.g., patient incontinent of stool or urine) could occur.

   iii. Wear gloves with fit and durability appropriate to the task.

      1. Wear disposable medical examination gloves for providing direct patient care.

      2. Wear disposable medical examination gloves or reusable utility gloves for cleaning and disinfecting the environment or medical equipment.

   iv. Remove gloves after contact with a patient and/or the surrounding environment (including medical equipment) using proper technique to prevent hand contamination.

   v. Do not wear the same pair of gloves for the care of more than one patient.

   vi. Do not wash gloves for the purpose of reuse as this practice has been associated with transmission of pathogens.

   vii. Change gloves during patient care if the hands will move from a contaminated body site (e.g., perineal area) to a clean body site (e.g., face).

c. *Gowns*

   i. Wear a gown providing 360-degree coverage to protect skin and prevent soiling and/or contamination of clothing during procedures and patient care activities when contact with blood, body fluids, secretions, or excretions or other potentially infectious material can be reasonably anticipated.

   ii. Wear a gown providing 360-degree coverage for direct patient contact if the patient has uncontained secretions or excretions.

   iii. Carefully remove gown to avoid contamination of clothing and perform hand hygiene before leaving the patient's environment.

   iv. Do not reuse gowns, even for repeated contact with the same patient.

   v. Routine donning of gowns upon entry into a high-risk unit (e.g., ICU, NICU) is not indicated.

d. *Medical Face Masks, Face Shields, N95 respirators and PAPR/CAPR*

   i. Use the appropriate PPE to protect the mucous membranes of the eyes, nose and mouth during procedures and patient-care activities that are likely to generate splashes or sprays of blood, body fluids, secretions or excretions. Select masks, goggles, face shields, and combinations of each according to the anticipated needs for the task to be performed.

   ii. When a medical face mask is required, it must be put on before entering the patient's room.

   iii. N95 Respirators and PAPR/CAPR (See Aerosol Transmissible Disease (ATD)

Exposure Control Plan)

1. During aerosol-generating procedures (e.g., bronchoscopy, suctioning of the respiratory tract [if not using in-line suction catheters], endotracheal intubation) in patients who are not suspected of being infected with an agent for which respiratory protection is otherwise recommended (e.g. *M. tuberculosis*, SARS, seasonal influenza, or hemorrhagic fever viruses), wear one (1) of the following: a face shield that fully covers the front and sides of the face, or a medical face mask and goggles (in addition to gloves and a gown providing 360-degree protection).

iv. Medical Face Masks

1. The following procedure should be observed when placing, wearing, and removing a mask:
    a. Put the mask on before donning gown and/or gloves.
    b. Place the mask over both the nose and the mouth and pull down under the chin.
    c. Arrange the top strings to pass over the top of the ears and the lower strings to pass at the neckline before securing if wearing a surgical mask; and secure earloops behind both ears if wearing a procedure mask.
    d. Change the mask as soon as it becomes moist or soiled.
    e. When removing the mask, remove gloves first if worn. Then, untie the lower strings and then the upper strings if surgical mask worn or remove earloops from both ears if procedure mask worn.
    f. Do not lower the mask around the neck and then reuse it.
    g. Use the mask only once and discard it in to the trash.

3. **Respiratory Hygiene/Cough Etiquette** *(See Respiratory Hygiene/Cough Etiquette policy for further information).*

a. Measures are implemented to contain respiratory secretions in patients or other individuals who have signs and symptoms of a respiratory infection upon entering the healthcare setting. These measures include:

i. Educate caregivers, patients and visitors on respiratory hygiene/cough etiquette.

ii. Posting signs at entrances and in strategic places (e.g., elevators, cafeterias) within ambulatory and inpatient settings with instructions to patients and other persons with symptoms of a respiratory infection to cover their mouths/noses when coughing or sneezing, use and dispose of tissues, and perform hand hygiene after hands have been in contact with respiratory secretions using alcohol-based handrubs or soap and water.

iii. Providing tissues and no-touch receptacles (e.g., foot-pedal operated lid or open, plastic-lined wastebasket) for disposal of tissues.

iv. During periods of increased prevalence of respiratory infections in the community, offer masks to coughing patients and other symptomatic persons (e.g., persons who accompany ill patients) upon entry into the facility or medical office and encourage them to maintain spatial separation, ideally a distance of at least 6 feet, from others in common waiting areas.

4. **Patient Placement**
   a. The potential for transmission of infectious agents is included in patient placement decisions. Place patients who pose a risk for transmission to others (e.g., uncontained secretions, excretions or wound drainage, infants with suspected viral respiratory or gastrointestinal infections) in a single-patient room when available.

   b. Consider the proximity of non-infectious, immunocompromised/immunosuppressed patient placement (e.g., oncology patients) to other patients who may be colonized and/or infected with infectious agents.

   c. Review transmission-based precautions section below regarding cohorting patients as needed.

   d. Elements to consider when deciding patient placement:
      i. Route(s) of transmission of the known or suspected infectious agent
      ii. Risk factors for transmission in the infected patient
      iii. Risk factors for adverse outcomes resulting from a healthcare-associated infection (HAI) in other patients in the area or room being considered for patient placement
      iv. Availability of single-patient rooms
      v. Patient options for room-sharing (e.g., cohorting patients with the same infection)

5. **Patient-Care Equipment and Instruments/Devices**
   a. Follow established policies and procedures for containing, transporting, and handling patient care equipment and instruments/devices that may be contaminated with blood or body fluids.

   b. Remove organic material from critical and semi-critical instrument/devices, using hospital-approved cleaning agents according to manufacturer's written instructions for use (MIFU) to allow for subsequent high-level disinfection and/or sterilization.

   c. Non-critical movable medical equipment must be cleaned and disinfected using EPA-registered, hospital-approved disinfectants in accordance with MIFU before use on another patient (e.g., commodes, intravenous pumps and ventilators, computer keyboards, phones, glucometer, etc.)

   d. PPE (e.g. gloves, gown providing 360-degree coverage) will be worn (according to the level of anticipated contamination) when handling patient-care equipment and instruments/devices that are visibly soiled or may have been in contact with blood or body fluids.

   e. Ensure that single-use items are discarded properly or placed in appropriate container for return to third party reprocessor or back to the manufacturer (e.g., pulse oximeters).

   f. Disposable articles contaminated with blood will be discarded in red bags labeled "Biohazardous Waste". Double bagging is not necessary unless the bag is contaminated, punctured or torn, or needed for strength. *Refer to Biohazardous Waste policy for further information.*

6. **Care of the Environment**
   a. Follow established policies and procedures for routine and targeted cleaning and disinfection of environmental surfaces as indicated by the level of patient contact and degree of soiling.
   b. Clean and disinfect surfaces that are likely to be contaminated with pathogens, including those in close proximity to the patient (e.g., bed rails, over bed tables, call bells) and frequently touched surfaces in the patient care environment (e.g., doorknobs, surfaces in and surrounding toilets in patients' rooms) on a more frequent schedule compared to that of other surfaces (e.g. horizontal surfaces in waiting rooms).
   c. Environment Protection Agency (EPA)-registered, hospital-approved disinfectants that have microbicidal (e.g., those with a kill claim) activity against the pathogens most likely to contaminate the patient-care environment will be used in accordance with MIFU. All disinfectants are to be approved by the Infection Prevention and Control Committee.
      i. Example: environment of a patient with *C. difficile* infection will require approved sporicidal cleaner.
   d. For areas providing care to pediatric patients, toys will be cleaned and disinfected at regular intervals. The following principles will be considered:
      i. Select play toys that can be easily cleaned and disinfected.
      ii. Do not permit use of stuffed furry toys if they are shared.
      iii. Clean and disinfect large stationary toys (e.g., climbing equipment) between use and whenever visibly soiled.
      iv. If toys are likely to be mouthed, rinse with water after disinfection; alternatively wash in a dishwasher.
      v. When a toy requires cleaning and disinfection, do so immediately or store in a designated labeled container separate from toys that are clean and ready for use.
   e. Multi-patient use electronic equipment and devices, including those items that are used by patients, those used during delivery of patient care, and mobile devices that are moved in and out of patient rooms frequently (e.g., movable medical equipment) should be cleaned and disinfected with an EPA-registered, hospital-approved disinfectant after each patient use and when visibly soiled.
   f. When possible, implement patient-dedicated non-critical equipment. In order to prevent waste, limit the amount of supplies taken into a patient's room to what is needed for patient care.

7. **Patient Medications**
   a. All medications that are patient-specific should be kept in a secure location for that patient (e.g., locked box in room, secure Pyxis drawer).

8. **Textiles and Laundry**
   a. Soiled textiles, including bedding, towels, and patient clothing may be contaminated with pathogenic microorganisms. The risk of disease transmission can be minimized by

handling soiled items in a safe manner.

b. Handle used textiles and linen with minimum agitation to avoid contamination of air, surfaces and persons.

c. Avoid contact with clothing when handling soiled items.

d. Laundry chutes, if used, will be maintained in a manner to minimize dispersion of aerosols from contaminated laundry. Avoid placing loose linen and textiles into the laundry chutes.

9. **Dishware and Utensils**

   a. The combination of hot water and detergents used in dishwashers is sufficient to decontaminate/sanitize dishware and eating utensils. If adequate resources for cleaning utensils and dishwashers are not available, disposable products may be used.

10. **Waste Disposal**

    a. Disposable items (including all types of masks) may be discarded in the regular trash unless they are classified as medical or biohazardous waste.

    b. Most articles do not need to be labeled as biohazardous when they are removed from the room or cubicle unless they are contaminated with biohazardous waste.

    c. Articles which are contaminated with biohazardous waste material must be bagged (or in the case of sharp items, contained in leak-proof, puncture-resistant containers) as biohazardous in order to prevent inadvertent exposures to other personnel and contamination of the environment.

    d. Generally, a single bag is adequate if the article can be placed into the bag without contaminating the outside of the bag. Biohazardous waste must be placed in approved bags or in marked puncture-resistant sharps containers.

    e. Consider the use of appropriate PPE if there is a risk of exposure to blood and/or body fluids.

11. **Safe Injection Practices**

    a. The following applies to the use of needles, cannulas that replace needles, and intravenous delivery systems:

       i. Aseptic technique will be used to avoid contamination of sterile injection equipment.

       ii. Medications will not be administered from a syringe to multiple patients, even if the needle or cannula on the syringe is changed. Needles, cannula, and syringes are sterile, single-use items and are never to be reused for another patient or to access a medication or solution that might be used for a subsequent patient.

       iii. Fluid infusion and administration sets (e.g., intravenous bags, tubings and connectors) will be used for one patient only and disposed of appropriately after use. A syringe or needle/cannula is considered contaminated once it has been removed from packaging and used to enter or connect to a patient's intravenous infusion bag or administration set.

       iv. Single-dose vials for parenteral medications are to be used whenever possible.

       v. Medications from single-dose vials or ampules will not be administered to multiple patients or residual contents combined for later use.

vi. If multi-dose vials must be used, both the needle or cannula and syringe used to access the multi-dose vial must be sterile.

vii. Multi-dose vials will not be kept in the immediate patient treatment area and will be stored in accordance with the manufacturer's written recommendations. Discard if sterility is compromised or questionable.

viii. Bags or bottles of intravenous solution will not be used as a common source of supply for multiple patients.

12. **Infection Control Practices for Special Lumbar Puncture Procedures**

    a. Surgical masks will be worn to fully cover the nose and mouth when placing a catheter or injecting material into the spinal or subdural space (e.g., during myelograms, lumbar puncture and spinal or epidural anesthesia).

    b. Follow Lippincott Procedure for additional considerations.

Transmission-based Precautions

PROCEDURE/GENERAL INSTRUCTIONS

1. **Initiating and Discontinuing Transmission-based Precautions**

   a. Used in addition to Standard Precautions

   b. Does not require a written order from the physician.

      i. Should be initiated by the nurse as soon as an infectious diagnosis is suspected or discovered, or multi-drug resistant organisms (MDROs) are reported, in accordance with Appendix A (see attached).

      ii. For the patient who appears to have a disease requiring Contact, Airborne, or Droplet Precautions, it is important to institute the appropriate precautions immediately. Do not wait for confirmation of the diagnosis.

      iii. Patients with wounds, drainage that cannot be covered or contained, or rashes of unknown origin should be in Contact Precautions regardless of the presence of MDRO.

      iv. The appropriate sign should be posted on the patient's door and the physician notified.

      v. Initiation of transmission-based precautions should be documented in the patient's electronic medical record.

         1. The Patient Isolation Status alert is auto-populated on the patient banner in the electronic medical record with a completed isolation order.

      vi. Modification of transmission-based precautions may be made at the discretion of the Infection Preventionist.

   c. Transmission-based precautions can be discontinued in accordance with the duration of precautions noted in Appendix A.

      i. The Infection Preventionist has the authority to initiate or discontinue transmission-based precautions based on patient record review and assessment.

ii. The Infection Preventionist may be consulted if there are any questions.

iii. Discontinuation of precautions should be documented in the patient's electronic medical record.

iv. When a patient on transmission-based precautions is being discharged or transferred to another room, do not remove the door sign until the Environmental Services department has completed thorough and proper cleaning and disinfection. The sign is then removed.

2. **Placement of Patients**

a. Placement will depend on the mode of transmission of the disease or infection, availability of private/single patient rooms, airborne infection isolation rooms (AIIR) and the condition of the patient.

b. When single-patient rooms are in short supply, apply the following principles for making decisions on patient placement.

i. Prioritize patients with conditions that may facilitate transmission of infectious agents (e.g., uncontrolled drainage, stool incontinence) for single-patient room placement.

ii. If a single patient room is unavailable, the infected or colonized patients should be placed/cohorted with appropriate roommates in cubicle isolation after collaboration with infection prevention and control.

iii. Generally, infected patients should not share a room with a patient who is likely to become infected and in whom the consequences of infection are likely to be severe. Such patients include those who are immunocompromised, immunosuppressed or who are about to undergo extensive surgery with insertion of invasive lines or prosthetic devices.

iv. When an infected patient shares a room with a non-infected patient, both patients must take measures to prevent the spread of infection by exhibiting good personal hygiene.

v. In general, patients infected or colonized with the same organism may share a room. Such grouping or cohorting of patients may be necessary during outbreaks when private/single patient rooms may not be readily available.

3. **Airborne Infection Isolation Rooms (AIIR) (Negative Air Pressure Rooms)**

a. Patients placed in Airborne Precautions should be placed in an AIIR with the recommended ventilation/air change requirements. If an AIIR is not available, a high-efficiency particulate air (HEPA) filter scrubber can be used in the room with the door closed until an AIIR becomes available.

b. Each ministry have designated identified as AIIR with 100% air exhausted to the outdoors and a minimum of 6 air changes per hour.

i. Appendix B lists the AIIR in each ministry.

ii. These rooms are monitored at least quarterly by Plant Operations/Facilities Engineering and daily when in use.

    c. Airflow data are kept on file by Plant Operations/Facilities Engineering.

    d. Should readings fall below established threshold levels, it is the responsibility of Plant Operations/Facilities Engineering to service and correct the air flow/negative pressure differentials.

4. **Transmission-based Precaution Signs**

    a. Standardized pre-printed signs will be used for transmission-based precautions.

    b. These must be posted outside the patient's door to provide instructions to caregivers, providers and visitors before entering the room.

5. **Transportation of Patients**

    a. When it becomes necessary to transport a patient on precautions to another area of the hospital, appropriate procedure mask should be placed on the patient to reduce the risk of disease transmission.

        i. Airborne Precautions: Procedure mask to cover nose and mouth if tolerated.

        ii. Contact Precautions: Clean patient gown, impervious wound dressing, cover with sheet

        iii. Droplet Precautions: Procedure mask, clean gown

    b. These barriers should remain in place for the entire period the patient is out of the isolation room. When these barriers are removed for purposes of procedural necessity, healthcare workers should be protected with their own appropriate barriers.

    c. The transport vehicle should be covered with a clean sheet or blanket.

    d. Personnel transporting the patient generally need not wear protective barriers such as gloves, masks, or gown.

6. **Patient Records**

    a. Patient record-keeping documents should not be allowed to become contaminated in the care of the patient. These documents should not be placed on the patient's bed or bedside table unless a protective barrier is used (e.g., a clean sheet). Gloves should be removed and hand hygiene performed before touching the documents.

7. **Food Trays, Dishes, Glasses, Cups, Eating Utensils**

    a. No special precautions are needed for these items and reusable food trays can be used for patients in most types of transmission-based precautions

    b. Additional measures may be indicated, follow ministry specific risk assessments and procedures. Some may include:

        i. Use of disposable trays

        ii. Tray covering

8. **Linen and Laundry**

    a. Soiled linen should be placed in the soiled linen hamper and handled according to Standard Precautions.

9. **Patient Care Equipment**

    a. As needed, dedicate the use of non-critical patient care equipment as single-patient use or patient specific (e.g., stethoscopes, sphygmomanometer or blood pressure cuff, bedside commodes, thermometers, etc.).

b. All reusable equipment will be handled, cleaned and disinfected according to hospital policy before use on another patient.

c. Disposable equipment should be discarded.

10. **Room Cleaning and Reuse**

    a. All environmental surfaces and frequently touched surfaces (e.g. patient care items, bedside equipment, door handles, countertops, sinks, bedrails, etc.) should be cleaned and disinfected daily and as needed using an EPA-registered, hospital-approved disinfectant.

    b. Environmental Services caregivers should wear the appropriate PPE as indicated by the Precaution sign on the patient's door and should contact the assigned nurse if there are any questions prior to entering.

    c. Partition curtains should be changed per ministry standard work.

    d. No wait time between admissions is required if the MIFU for cleaning and disinfection is followed. See Airborne Precautions section below for additional measures.

    e. Terminal cleaning procedures are performed in all inpatient rooms when a patient is discharged/ transferred or precautions is discontinued.

11. **Patient and Visitor Education**

    a. Explain to patients and visitors the reason for the precautions.

    b. Visitors should use the precautions for caregivers outlined in this policy, and perform hand hygiene (wash hands with soap and water or use alcohol-based hand rub) before entering and upon leaving the patient's room.

    c. Provide instructions on respiratory hygiene/cough etiquette (e.g., covering nose and mouth with a tissue when coughing or sneezing, disposing tissue in the trash, and perform hand hygiene).

    d. Provide education on the importance of patient hand hygiene to decrease the risk of self-contamination.

    e. Document education provided in the patient's electronic health record.

12. **Ambulation**

    a. Ambulation of a patient on transmission-based precautions is allowed per the Infection Prevention risk assessment.

13. **Infections and Conditions Not Otherwise Listed**

    a. Should a patient be admitted with infections, conditions, or clinical syndromes not otherwise listed under the three transmission-based precautions, contact the Infection Prevention and Control Department for recommendations.

TRANSMISSION-BASED PRECAUTIONS

AIRBORNE PRECAUTIONS

1. **Use Airborne Precautions:**

a. Used in addition to Standard Precautions.

b. For any patient known or suspected to have an illness transmitted by the airborne route.

c. Refer to Appendix A attached for a list of suspected or confirmed diseases/ microorganisms that should be placed on Airborne Precautions and for the proper duration of precautions.

d. Each ministry will have a list of specific AIIR.

2. **Patient Placement**

a. Place in a private airborne infection isolation room (AIIR).

b. Door(s) should be kept closed when not required for entry and exit to minimize airflow to the corridor.

c. Place Airborne Precaution sign outside patient's room.

d. If an AIIR is not available, contact Infection Prevention.

e. The use of a private/single patient room with the door closed is an option with the use of a HEPA filtered scrubber until an AIIR becomes available.

3. **Caregiver Respiratory Protection**

a. *Refer to Respiratory Protection: N95 and PAPR policy and/or Aerosol transmissible Disease (ATD) Exposure Control Plan*

b. Wear the appropriate respiratory protection (e.g., PAPR/CAPR or fit-tested NIOSH-approved N95 or higher level respirator) when entering the room of a patient on Airborne Precautions.

i. In situations where there is a N95 respirator supply shortage, caregivers may reuse or extend the use of disposable N95 respirators in consultation with the local health department, California Department of Public Health (CDPH), and California Occupational Safety and Health Administration (CalOSHA).

ii. A higher level of respiratory protection is required during high-hazard aerosol-producing procedures (e.g., bronchoscopy and cough inducing procedures) for all caregivers during the procedure and for 1 hour after the procedure is completed.

c. Respiratory protection is required before entering the room and is removed after leaving room.

d. Caregivers are not to enter the rooms of patients known or suspected to have measles (rubeola) or varicella (chickenpox), or disseminated zoster if susceptible to these infections. Contact Caregiver Health Services and/or Infection Prevention and Control departments for additional concerns.

e. Some diagnoses may require other transmission-based precautions in addition to airborne (e.g., contact/airborne). Please refer to Appendix A for more information regarding these circumstances.

f. Perform hand hygiene immediately prior to entry and on exiting the room.

4. **Visitor Protection and Personal Protective Equipment**

a. All visitors should practice hand hygiene prior to entering and upon exiting the patient's room.

b. Visitors should wear a procedure mask to enter patient's room who is on Airborne Precautions.

c. In outbreak situations or novel pathogen transmission, enforce visitor restrictions as directed by State and County regulations.

5. **In the event that an AIIR is not available due to an outbreak or exposure involving large numbers of patients who require Airborne Precautions:**

a. Consult Infection Prevention for patient placement to determine the safety of alternative rooms/settings that do NOT meet engineering requirements for an AIIR.

b. Use temporary portable solutions (e.g., HEPA filter scrubber vented to the outdoors away from air intakes) to create a temporary AIIR.

c. Once identified, place the patient in an AIIR as soon as possible.

i. If an AIIR is not available, place a procedure mask on the patient to cover nose and mouth and place the patient in a private/single patient room with a portable HEPA filter scrubber.

d. Once the patient leaves the room, the room should remain vacant or an approved N95 respirator should be worn for the appropriate time, generally one hour, to allow for a full air change.

e. Instruct patients with a known or suspected airborne infection to wear a procedure mask to cover nose and mouth and observe Respiratory Hygiene/Cough Etiquette when in common areas or in a room that does not have negative air flow.

f. Cohort patients who are presumed to have the same infection (based on clinical presentation and diagnosis when known) in areas of the facility that are away from other patients, especially patients who are at increased risk for infection (e.g., immunocompromised/immunosuppressed patients). Consult Infection Prevention.

6. **Patient Transport**

a. Limit the movement and transport of the patient from the AIIR to medically-necessary procedures whenever possible

b. When transport or movement is necessary, minimize patient dispersal of airborne pathogens by placing a procedure mask on the patient to cover the mouth and nose, if tolerated.

c. Transport caregivers should not wear PPE during patient transport unless previously approved by Infection Prevention.

d. Notify the receiving department that Airborne Precautions are necessary.

DROPLET PRECAUTIONS

1. **Use Droplet Precautions:**

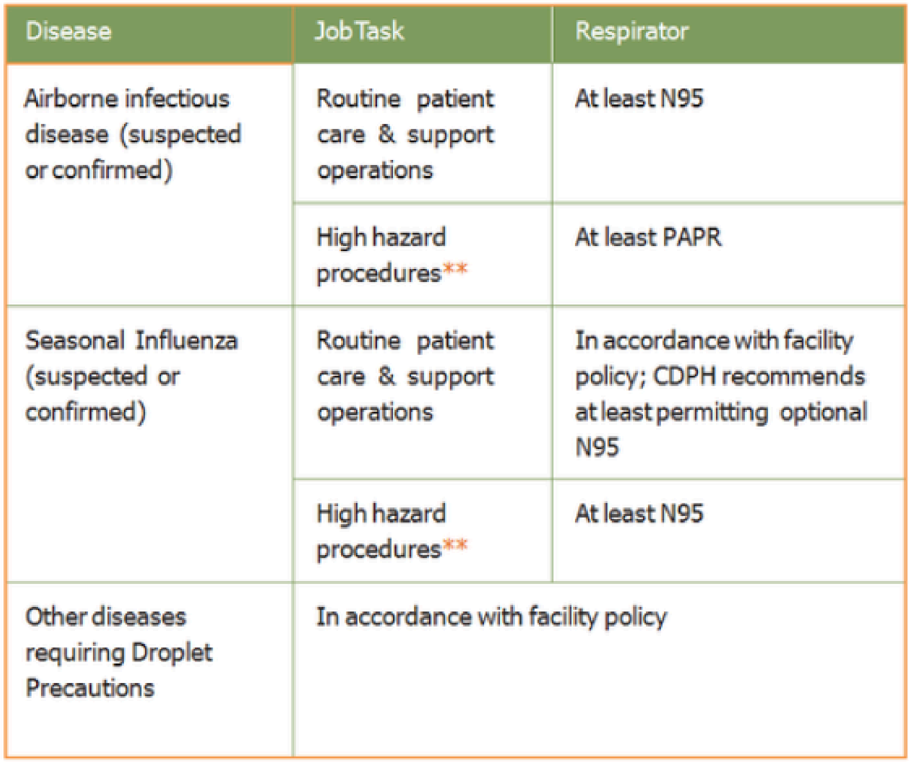
a. Used in addition to Standard Precautions.

b. For patients known or suspected to have illnesses transmitted by large particle respiratory droplets (larger than 5 mm in size) that is generated by a patient who is coughing, sneezing, or talking, or during performance of certain procedures.

c. Refer to Appendix A, attached, for a list of suspected or confirmed diseases and/or conditions that would require Droplet Precautions and for the proper duration of precautions.

2. **Patient Placement**
    a. Place patient in a private/single patient room (an AIIR is not required) as available.
    b. Cohorting patients:
        i. Prioritize patients who have excessive cough and sputum production for private/single patient room placement.
        ii. When cohorting is not achievable, maintain spatial separation of at least six feet between the infected patient and other patients and visitors.

3. **Caregiver Protection and Personal Protective Equipment (PPE)**
    a. In addition to Standard Precautions, always wear a procedure mask to cover nose and mouth (e.g., regular surgical or procedure mask with face shield, goggles) when working within six feet of the patient.
        i. Eye protection with a hospital-approved face shield or goggles should be used based on risk of exposure to the eyes.
        ii. Procedure masks worn for Transmission-based Precautions should be discarded and not reused upon exiting the patient's room.
    b. Follow the CDC's sequence of donning and doffing of PPE. See link above.
        i. Perform hand hygiene between steps if hands become contaminated and immediately after removing all PPE.
    c. For seasonal influenza (suspected or confirmed), all caregivers with direct patient contact have the option to wear a NIOSH approved, fitted tested N95 respirator or higher level respirator (e.g. PAPR/CAPR).
        i. At a minimum, NIOSH-approved fit tested N95 respirators are required when caring for seasonal influenza patients having high hazard cough inducing procedures (e.g., bronchoscopy) during the procedure and for one hour after procedure completion.



Disease	Job Task	Respirator
Airborne infectious disease (suspected or confirmed)	Routine patient care & support operations	At least N95
	High hazard procedures**	At least PAPR
Seasonal Influenza (suspected or confirmed)	Routine patient care & support operations	In accordance with facility policy; CDPH recommends at least permitting optional N95
	High hazard procedures**	At least N95
Other diseases requiring Droplet Precautions	In accordance with facility policy	

California Department of Public Health, Occupational Health Branch AUGUST 2015

4. **Visitor Protection and Personal Protective Equipment**
   a. All visitors should practice hand hygiene prior to entering and upon exiting the patient's room.
   b. Visitors are to wear a procedure mask to cover the nose and mouth for patients on Droplet Precautions unless exposed prior to hospitalization.
   c. In outbreak situations or the occurrence of novel pathogen transmission, visitor restrictions will be enforced as directed by State and County regulations.

5. **Patient Transport**
   a. Limit the movement and transport of the patient out of their room to medically-necessary procedures that cannot be performed in their room.
   b. If transport or movement is necessary, minimize patient dispersal of droplets by placing a procedure mask the patient to cover nose and mouth if tolerated. Otherwise have the patient cover their nose and mouth with a tissue.
   c. Transport caregiver should not wear PPE during transport of the patient unless providing direct patient care or directed to do so by Infection Prevention.
   d. Notify the receiving department that the patient that Droplet Precautions are necessary.

CONTACT PRECAUTIONS

1. **Use Contact Precautions:**
   a. Used in addition to Standard Precautions.
   b. For patients known or suspected to be infected or colonized with epidemiologically important/significant microorganisms that can be transmitted by direct/indirect contact

with the patient (e.g., hand or skin-to-skin contact that occurs when performing patient care activities that require touching the patient) or with environmental surfaces or patient care items in the patient's environment.

c. Refer to Appendix A for a list of suspected or confirmed diseases and/or conditions that requires patients to be placed in Contact Precautions and the proper duration of precautions.

    i. Epidemically significant organisms will require Contact Precautions.

    ii. In endemic situations, based on ministry specific risk assessment, Standard Precautions can be used for some MDROs (e.g., MRSA, VRE, ESBL).

    iii. Contact Precautions should be implemented for patients with large open wounds that cannot be covered and/or drainage that cannot be contained, regardless of microbiological culture results.

    iv. Any patients with rashes of unknown origin should be placed in Contact Precautions.

2. **Patient Placement**

    a. Place patients in a private/single patient room, if available. Place a Contact Precaution sign outside the patient's room.

3. **Caregiver Protection and Personal Protective Equipment (PPE)**

    a. In addition to Standard Precautions, wear gloves and gown with 360-degree coverage when there is a risk of self or clothing having direct contact with the patient, potentially contaminated environmental surfaces or items.

    b. Caregivers may enter a Contact Precautions room after performing hand hygiene with soap and water or an alcohol-based hand rub.

    c. Don PPE when entering a patient's room based on the anticipated interaction with the patient or their environment.

    d. While providing care of a patient, change gloves after having contact with infectious material that may contain high concentrations of microorganisms (e.g., fecal material and wound drainage).

    e. Remove/doff PPE before leaving the patient's room and perform hand hygiene immediately.

    f. After removal/doffing of PPE and performing hand hygiene, ensure that hands and clothing do not touch potentially contaminated environmental surfaces or items in the patient's room prior to exiting the patient's room.

    g. Follow CDC's sequence of donning and doffing of PPE. Refer to the link above.

        i. Perform hand hygiene between each step if hands become contaminated and immediately after removing all PPE.

4. **Visitor Protection and Personal Protective Equipment**

    a. All visitors should practice hand hygiene prior to entering and upon exiting the room.

    b. Visitors should wear a gown providing 360-degree coverage and gloves for contact with patient or patient's environment.

5. **Patient Transport**

a. Limit the movement and transport of the patient from the room to medically-necessary procedures and tests that cannot be completed in their room.

b. When transport or movement of the patient is necessary, verify that all secretions and excretions are contained (e.g., wounds are covered). The patient should perform or be assisted with hand hygiene.

c. Notify the receiving department that the patient is on Contact Precautions.

d. When transport is necessary, and no patient contact is anticipated en route, the transport caregiver should remove PPE and perform hand hygiene prior to patient transport. Don clean PPE on arrival to the receiving department.

e. If direct patient care is needed during transport (e.g., bagging a ventilated patient),

    i. The transport caregiver wearing the PPE to perform patient care en route, should **NOT** touch anything in the environment, and they MUST be accompanied by another caregiver NOT in PPE who will open doors and push elevator buttons.

    ii. If the patient's bed and/or other equipment such as an IV pole accompany the patient on the transport, then bedrails and equipment should be disinfected with an EPA-registered hospital approved disinfectant prior to transport.

f. The testing or procedure area should be thoroughly cleaned and disinfected with and EPA registered, hospital approved disinfectant after the patient leaves the area.

CONTACT ENTERIC PRECAUTIONS

1. **Use Contact Enteric Precautions:**

    a. Used in addition to Standard Precautions.

    b. For patients with diarrhea of unknown cause, known or suspected *C. difficile* infections and/or certain gastroenteritis conditions.

    c. Refer to Appendix A for a list of suspected or confirmed diseases and conditions for which patients should be placed in Contact Enteric Precautions and for the proper duration of precautions.

2. **Patient Placement**

    a. Place patient in a private room/single patient room if available.

    b. It is not necessary to keep the door closed.

    c. Place Contact Enteric Precautions sign outside patient's room.

3. **Caregiver Protection and Personal Protective Equipment (PPE)**

    a. In addition to Standard Precautions, wear gloves and a gown providing 360-degree coverage for direct contact with the patient, potentially contaminated environmental surfaces or items near the patient.

    b. While providing care for a patient, change gloves after having contact with infectious material that may contain high concentrations of microorganisms (e.g., fecal material).

    c. Remove PPE before leaving the patient's room and wash hands with soap and water with friction for 15-20 seconds. Do not use alcohol-based hand rub.

    d. After removal of PPE, perform hand hygiene, ensure that hands and clothing do not touch potentially contaminated environmental surfaces or items in the patient's room prior to exiting the patient's room.

   e. Follow CDC's sequence of donning and doffing of PPE. See the link above.

      i. Perform hand hygiene between steps if hands become contaminated and immediately after removing/doffing all PPE.

   f. Use an EPA-registered, hospital approved sporicidal agent (e.g., bleach) to clean and disinfect patient care areas, high touch surfaces, and movable medical equipment. Verify with the equipment MIFU that bleach can be used for cleaning and disinfection.

4. **Visitor Protection and Personal Protective Equipment**

   a. All visitors should practice hand hygiene prior to entering and upon exiting the room.

   b. Visitors are to wear a gown with 360-degree coverage and gloves for contact with the patient and/or the environment.

5. **Patient Transport**

   a. Limit the movement and transport of the patient out of the room to medically-necessary procedures and tests that cannot be performed in the room.

   b. When transport or movement is necessary, ensure that all secretions and excretions are contained. (e.g., wounds are covered). The patient should perform hand hygiene or be assisted with hand hygiene to prevent contamination of environmental surfaces.

   c. Notify the receiving department that the patient is on Contact Enteric Precautions.

   d. When transport is necessary, and no patient contact is anticipated, transport caregivers should remove PPE and perform hand hygiene prior to patient transport. Don clean PPE on arrival to the receiving department.

   e. If direct patient care is needed during transport (e.g., bagging a ventilated patient),

      i. Transport caregiver who MUST have patient contact (e.g., bagging a ventilated patient, etc.), should wear PPE to perform patient care en route. The transport caregiver wearing the appropriate PPE to perform patient care should NOT touch anything in the environment, and they MUST be accompanied by another caregiver NOT wearing PPE who will open doors and push elevator buttons.

   f. If the patient's bed and/or other equipment such as an IV pole that will accompany the patient on the transport, should be cleaned and disinfected with an EPA-registered, hospital approved sporicidal agent (e.g., bleach) prior to transport.

   g. The testing or procedure area should be cleaned and disinfected thoroughly an EPA-registered, hospital approved sporicidal agent after the patient leaves the area.

REFERENCE(S)/RELATED POLICIES

Related Documents and Policies

- Donning and Doffing Personal Protective Equipment Policy
- Hand Hygiene Policy
- Biohazardous Waste Policy
- Respiratory Hygiene and Cough Etiquette Policy

- Movable Medical Equipment Policy
- Germicides, Selection and Use of Policy
- Respiratory Protection: N95 and PAPR
- **References**
- Siegel JD, Rhinehart E, Jackson M, Chiarello L, Healthcare Infection Control Practices Advisory Committee. Management of Multidrug-Resistant Organisms in Healthcare Settings, 2006 [PDF - 553 KB] (https://www.cdc.gov/infectioncontrol/pdf/guidelines/mdro-guidelines.pdf). Am J Infect Control, 2007 Dec 35 (10 Suppl 2):S165-93. https://www.cdc.gov/infectioncontrol/guidelines/mdro/index.html Online version last reviewed November 5, 2015.
- Siegel JD, Rhinehart E, Jackson M, Chiarello L, Healthcare Infection Control Practices Advisory Committee. 2007 Guideline for Isolation Precautions: Preventing Transmission of Infectious Agents in Healthcare Settings [PDF - 1.42 MB] Am J Infect Control. 2007 Dec 35(10 Suppl 2)S65-164. (https://www.cdc.gov/infectioncontrol/pdf/ guidelines/isolation-guidelines-H.pdf Last updated May 2022).
- California Department of Public Health. Respirator Use in Health Care: Cal/OSHA ATD Standard. Title 8 CCR; Section 5199. (https://www.cdph.ca.gov/Programs/CCDPHP/DEODC/OHB/Pages/ATDStd.aspx)
- Centers for Disease Control and Prevention. Guidance for Control of Infections with Carbapenem-Resistant or Carbapenemase-Producing Enterobacteriaceae in Acute Care Facilities [PDF - 381 KB] MMWR 2009 Mar 20:58 (10):256-60. Facility Guidance for Control of Carbapenem-resistant Enterobacteriaceae (CRE) - CRE Toolkit https://www.cdc.gov/hai/pdfs/cre/cre-guidance-508.pdf. Updated November 2015
- L. Silvia Munoz-Price, David B. Banach, Gonzalo Bearman, Jane M. Gould, Surbhi Leekha, Daniel J. Morgan, Tara N. Palmore, Mark E. Rupp, David J. Weber and Timothy L. Wiemken Isolation Precautions for Visitors. Infection Control & Hospital Epidemiology, Available on CJO 2015 doi:10.1017/ice.2015.67
- N95 Respirators, Surgical Masks, Face Masks, and Barrier Face Coverings | FDA

Approval Signatures

Step Description	Approver	Date
Regional Site Adminsitrator	Wen Yun Chang: Senior Business Analyst	12/2022
Division CNO - South	Daniel Kelly: Chief Nursing Officer	12/2022
Exec Dir Clin Ops SoCal Reg	Kevin Streeter: Executive Director Clinical Operations	12/2022
Regional Site Adminsitrator	Wen Yun Chang: Senior Business Analyst	12/2022
Regional Policy Owner	Jacqueline Daley: Senior Director Infection Prevention	12/2022

Applicability

CA - Regional/Divisional

Standards

No standards are associated with this document

Safe Patient Handling – California Clinical Caregivers

California's Safe Patient Handling law Title 8 §5120 requires acute care hospitals to provide Safe Patient Handling equipment and live training on the available equipment on hire and annually.

Goal: Reduce injury risk for workers who move patients by using equipment that reduces forceful exertions.

Areas of Risk with Manual Patient Handling:

- **Repositioning:** boosting and turning – highest injury risk
- **Vertical transfers:** bed <-> chair bed <-> bedside commode
- **Lateral transfers:** bed <-> gurney gurney <-> imaging / OR table
- **Bariatric mobility**
- **Ambulation:** sit-to-stand, standing, catching falling patients

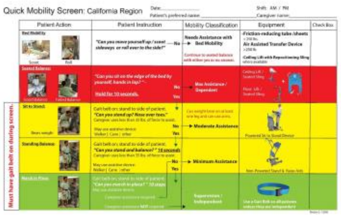
Registered Nurse is the Coordinator of Care – responsible for patient mobility assessment and documenting the patient's mobility status on admission and when there is a change in condition. RN is responsible for observation and direction of patient lifts and mobilization.

Best practice: All caregivers do Quick Mobility Screen before attempting to move patients.

Right to Refuse: Caregivers can refuse to lift, reposition, mobilize, or transfer a patient due to concerns about patient or worker safety or the lack of trained personnel or equipment. Report any concerns to supervisor. Do not use broken equipment – tag equipment and remove it from use. Notify BioMedical Engineering.

Quick Mobility Screen: Bed Mobility

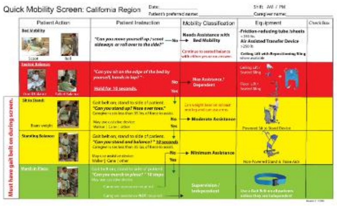
Needs Assistance vs. Independent Bed Mobility


Quick Mobility Screen: California Region
Patient Action
Patient Instruction
Mobility Classification
Equipment
Check Box
Needs Assistance with Bed Mobility
Max Assistance / Dependent
Moderate Assistance
Minimum Assistance
Supervision / Independent
Must have gait belt on during screen.

Step 1: Bed Mobility:
Can the patient
Roll side to side, scoot sideways & scoot up in bed?
NO = Needs Assistance.
Use bed controls and Anti-Friction sheet/tube or Air-Assisted Device (e.g. Hovermatt, AirTAP) for repositioning & lateral transfers

Quick Mobility Screen: Seated Balance

Safe sitting ability – able vs not able


Quick Mobility Screen: California Region

Step 2 : Seated Balance
Can the patient sit on the edge on the bed & maintain good balance with hands in lap x 10 seconds?
NO = Max Assist. Use a ceiling lift or floor lift with seated sling to transfer to chair / commode / wheelchair

Quick Mobility Screen: Sit to Stand*

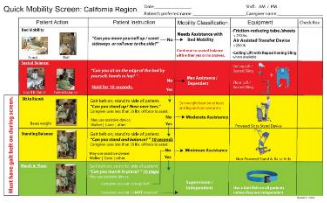
Safe standing ability

Quick Mobility Screen: California Region

Step 3 : Sit to Stand
Can the patient stand up with little to no assistance from one caregiver?
NO = Moderate Assist.
Use a powered sit to stand device, if patient can weight bear on at least one leg and use arms (if not, Max Assist)

Quick Mobility Screen: Standing Balance

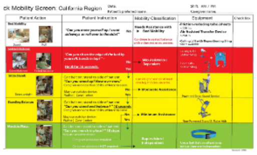
Safe static balance ability


Quick Mobility Screen: California Region

Step 4 : Can the patient stand and balance for 10 seconds with little to no assistance?
YES = Continue to march in place test
No = Consider Moderate Assist

Quick Mobility Screen: March in Place

Safe dynamic balance ability


ck Mobility Screen: California Region

Step 5 : Can the patient march 10 steps in place with little to no assistance?
NO = Minimum Assist. Use a non-powered stand and raise aid
YES = Supervised/Independent Use a gait belt unless the patient is independent

Status Active PolicyStat ID 16990002

Origination	09/2006	Owner	David Lane: Chief Compliance Officer
Last Approved	11/2024	Policy Area	Compliance
Effective	11/2024	Applicability	Providence Systemwide + PGC
Last Revised	11/2024	Departments	Posted on Internet
Next Review	11/2025		

PSJH-CPP-711 Fraud, Waste and Abuse Prevention and Detection

Executive Sponsor:	Erik Wexler, President/CEO
Policy Owner:	David Lane, VP/Chief Compliance Officer
Contact Person:	Karen J. Coleman, System Director Compliance Auditing & Monitoring

Scope:

This policy applies to Providence and its Affiliates (collectively known as "Providence")[i] and their caregivers (employees), employees of affiliated organizations; members of system, community ministry and foundation boards; volunteers; trainees; independent contractors; and others under the direct control of Providence (collectively referred to as workforce members). Providence educational institutions are excluded from this healthcare related policy.

☑ Yes ☐ No Is this policy applicable to Providence Global Center (PGC) caregivers?

This is a management level policy reviewed and recommended by the Policy Advisory Committee for approval by senior leadership which includes vetting by Executive Leadership Committee with final approval by the President, Chief Executive Officer or appropriate delegate.

Purpose:

This policy confirms Providence's commitment to prevent and detect fraud, waste and abuse (FWA) by providing workforce members detailed information regarding: (1) the federal False Claims Act; (2) federal laws and penalties pertaining to reporting and returning overpayments; (3) state laws and penalties pertaining to false claims; and (4) whistleblower protections under certain laws.

Definitions:

For purposes of applying this policy, the following definitions apply:

1. *Abuse:* includes actions that may, directly or indirectly, result in: unnecessary costs to the Medicare Program, improper payment, payment for services that fail to meet professionally recognized standards of care, or services that are medically unnecessary. Abuse involves payment for items or services when there is no legal entitlement to that payment and the provider has not knowingly and/or intentionally misrepresented facts to obtain payment. Abuse cannot be differentiated categorically from fraud, because the distinction between “fraud” and “abuse” depends on specific facts and circumstances, intent and prior knowledge, and available evidence, among other factors.
2. *Agents:* Anyone directly performing services on behalf of Providence.
3. *Caregiver:* Refers to all employees/workforce members of Providence.
4. *Claim:* As defined in the federal False Claims Act, a "Claim" includes any request or demand, whether under a contract or otherwise, for money or property which is made by a contractor, grantee, or other recipient, if the government provides any portion of the money or property, or will reimburse the requesting entity for any portion of the money or property, that is requested or demanded.
5. *False Claims Act (FCA):* The federal False Claims Act (31 USC 3729-33) makes it a crime for any person or organization to knowingly make a false record or file a false claim with the government for payment. "Knowingly" means that the person or organization:
    a. Knows the record or claim is false, or
    b. Seeks payment while ignoring whether the record or claim is false, or
    c. Seeks payment recklessly without caring whether the record or claim is false.
6. *Fraud:* is knowingly and willfully executing, or attempting to execute, a scheme or artifice to defraud any health care benefit program or to obtain (by means of false or fraudulent pretenses, representations, or promises) any of the money or property owned by, or under the custody or control of, any health care benefit program. (18 U.S.C. § 1347).
7. *Overpayment:* Funds that a person or organization receives or retains under Medicare or Medicaid/Medi-Cal to which the person or organization, after applicable reconciliation, is not entitled under those programs.
8. *Waste:* is the over-utilization of services, or other practices that, directly or indirectly, result in unnecessary costs to Medicare or a federal health program. Waste is generally not considered to be caused by criminally negligent actions but rather the misuse of resources.
Examples of potential FWA; this list is not conclusive:

Falsifying claims	Eligibility determination issues
Improper alteration of claim	Misrepresentation of medical condition
Incorrect coding	Failure to report third party liability

Double billing	Physical, mental, emotional, sexual abuse
Billing for services not provided	Neglect
Misrepresentation of services/ supplies	Discrimination
Improper substitution of services	Providing substandard care
Inaccurate cost reports	Providing medically unnecessary services
Kickback/Stark Law violations	Financial exploitation
Fraudulent credentials	Fraudulent recoupment practices
Embezzlement	Failure to refer for needed services
Under-utilization and over-utilization	Violations of Medicare's Conditions of Participation
Known retention of an overpayment	

9. *Whistleblower (Qui tam) Provision:* Allows a private person to bring a lawsuit on behalf of the government where the private person has information that the named defendant has knowingly submitted or caused the submission of false or fraudulent claims to the government.
10. *Workforce Members:* means caregivers, volunteers, trainees, interns, medical staff, students, independent contractors, vendors and all other individuals working at the ministry, whether they are paid by or under the direct control of the facility.

Policy:

It is the policy of Providence to comply with applicable federal and state laws and regulations pertaining to FWA in federal and state health care benefit programs and to disseminate information to its workforce members regarding such laws and regulations. Providence is committed to the diligent prevention and detection of FWA through its Board-approved Compliance Program Description and Standards/Code(s) of Conduct.

Requirements:

Providence will train and educate its workforce members and contractors as necessary to comply with the legal and regulatory requirements related to FWA and will work cooperatively with workforce members when problems are identified to resolve those problems as quickly as possible.

Providence will follow federal and state False Claims Acts, to educate new workforce members within 90 days of hire or engagement and will educate existing workforce members and contractors annually thereafter to the policies and procedures intended to meet those requirements. Providence will monitor education given to employees to verify this policy has been effectively implemented. Providence expects workforce members and contractors who are involved with creating and filing claims for payment for Providence services will only use true, complete and accurate information to make the claim. Billing for clinical trials will follow clinical trial billing protocols and will be submitted in accordance with federal requirements.

Providence will monitor and audit compliance with billing and coding requirements (through the Revenue Cycle department, Providence Health Plan and other appropriate departments) in order to detect errors and inaccuracies and will take appropriate actions to correct any issues causing billing inaccuracies. Providence will exercise reasonable diligence to identify and investigate any instances in which an overpayment may have been received. In all situations where overpayments are identified, Providence will report and return overpayments identified in a timely manner (i.e., no later than 60 days after identification and quantification) and in accordance with applicable federal and/or state requirements.

Providence divisions, ministries or facilities will create policies and procedures to comply with any applicable state-level False Claims Act requirements and will provide education to their existing workforce members and contractors on those policies and procedures and will train new workforce members upon hire or engagement.

Workforce members and contractors are expected and have a responsibility and duty to report any concerns about billing issues, a potential overpayment, or any other issue they feel is illegal or otherwise inappropriate, in accordance with the Code of Conduct. Concerns may be reported to the Providence Integrity Hotline at (888) 294-8455 or to the Integrity Hotline online reporting system. Potential overpayment issues should be brought immediately to the attention of the Department of Legal Affairs, Compliance and/or Revenue Cycle department.

Workforce members have the right to be protected against retaliation for good faith reporting of suspected wrongdoing or assisting in an investigation of possible wrongdoing. This commitment is expressed in our Code of Conduct and Non-Retaliation Policies. Providence expects workforce members and contractors to be familiar with the Standards/Code(s) of Conduct and other policies and to follow them.

Management is responsible for ensuring that workforce members are educated to the requirements of this policy and that the education is documented and producible upon audit. The form and extent of that training will be determined by the workforce member's function. Other workforce members will receive informational materials or awareness training.

Providence workforce members who do not follow this policy may be subject to disciplinary action up to and including termination of employment or contractual relationships.

A person who knows a claim was filed for payment in violation of the False Claims Act can file a lawsuit in Federal Court on behalf of the government, and in some cases, receive a reward for bringing original information about a violation to the government's attention.

Some states have a False Claims Act that allows a similar lawsuit in state court if a false claim is filed with the state for payment, such as under Medicaid or Workers' Compensation. Penalties are severe for violating the federal False Claims Act and may include repayment of up to three times the value of the false claim, significant fines per claim (e.g., 2024 fines range from $13,946 to $27,894 per claim) and/or imprisonment for 5 years. The amount is adjusted each year for inflation. In addition, individuals and entities can face administrative penalties such as exclusion from participating in federal and state-funded health care benefit programs, including Medicare and Medicaid.

Providence will notify impacted plan sponsors of any confirmed individuals or entities excluded from federal or state programs that may impact plan participants of the sponsor as applicable. Additionally, Providence will notify impacted plan sponsors of any confirmed reports to the Integrity Hotline Regarding Medicare Program noncompliance and/or fraud, waste and abuse violations that may impact plan participants of the sponsor as applicable.

References:

- Providence Code of Conduct
- Compliance Program Description
- PSJH-CPP-733 Non-Retaliation
- PSJH-CPP-736 Compliance Hotline Policy
- PSJH-CPP-735 Investigations Policy
- PSJH-CPP-741 Disclosure Program Policy
- PSJH-CPP-743 Compliance Reporting Obligations Policy
- Federal False Claims Act
- Deficit Reduction Act of 2005
- Federal Register/Adjustment of Civil Monetary Penalty Amounts for 2024
- Section 1128J(d) (reporting and returning overpayments) and Section 1909 of the Social Security Act
  (establishes liability to state for false or fraudulent claims)
- 42 C.F.R. Part 401, Subpart D Reporting and Returning of Overpayments
- State False Claims Acts Reviewed by the OIG
- CMS Medicare Managed Care Manual Chapter 21, Section 50
- Combating Medicare Parts C and D Fraud, Waste and Abuse Web-Based Training, January, 2019
- Office of Inspector General Fraud and Abuse Laws
- MLN Booklet - MLN4649244 Medicare Fraud

State	***Links to False Claims Legislation or Information***
Alaska	http://www.legis.state.ak.us/basis/statutes.asp#47.05.210
California	The False Claims Act, Cal. Gov't Code §§ 12650 et seq.
Idaho	https://legislature.idaho.gov/sessioninfo/2004/legislation/S1332/
Montana	http://www.falseclaimsact.com/wp-content/uploads/2013/02/Montana.pdf
New Mexico	https://www.nmag.gov/medicaid-fraud-control.aspx
Oregon	https://www.doj.state.or.us/consumer-protection/sales-scams-fraud/medicaid-fraud/
Texas	https://oig.hhsc.texas.gov/report-fraud
Washington	https://apps.leg.wa.gov/rcw/default.aspx?cite=74.66&full=true; https://apps.leg.wa.gov/rcw/default.aspx?cite=74.09

Applicability:

[i] For purposes of this policy, “Affiliates” is defined as any not-for-profit or non-profit entity that is wholly owned or controlled by Providence St. Joseph Health (PSJH), Providence Health & Services, St. Joseph Health System, Western HealthConnect, Kadlec, Covenant Health Network, Grace Health System, Providence Global Center*, NorCal HealthConnect, or is a not-for-profit or non-profit entity majority owned or controlled by PSJH or its Affiliates and bears the Providence, Swedish Health Services, St. Joseph Health, Covenant Health, Grace Health System, Kadlec, or Pacific Medical Centers names (includes Medical Groups, Home and Community Care, etc.). *Policies and/or procedures may vary for our international affiliates due to regulatory differences.

Approval Signatures

Step Description	Approver	Date
Policy Owner	David Lane: Chief Compliance Officer [CJ]	11/2024
Policy Contact	Karen Coleman: Director Compliance	11/2024

Applicability

AK - Credena Health, AK - Providence Alaska MC, AK - Providence Kodiak Island MC, AK - Providence Medical Group, AK - Providence Seward MC, AK - Providence St. Elias Specialty Hospital, AK - Providence Valdez MC, CA - Credena Health, CA - Healdsburg Hospital, CA - Petaluma Valley Hospital, CA - Physician Enterprise Northern, CA - Physician Enterprise Southern, CA - Providence Cedars-Sinai Tarzana MC, CA - Providence Holy Cross MC, CA - Providence LCM MC San Pedro, CA - Providence LCM MC Torrance, CA - Providence Mission Hospitals, CA - Providence Queen of the Valley Medical Center, CA - Providence Redwood Memorial Hospital, CA - Providence Saint John's Health Center, CA - Providence Saint Joseph MC, Burbank, CA - Providence Santa Rosa Memorial Hospital, CA - Providence St. Joseph Hospital - Eureka, CA - Providence St. Joseph Hospital Orange, CA - Providence St. Jude Medical Center, CA - Providence St. Mary Medical Ctr Apple Valley, MT - Credena Health, MT - Providence St. Joseph MC, Polson, MT - St. Patrick Hospital, NM - Covenant Hobbs Hospital, OR - Credena Health, OR - Providence Ctr for Medically Fragile Children, OR - Providence Health Oregon Labs, OR - Providence Hood River Memorial Hospital, OR - Providence Medford MC, OR - Providence Medical Group, OR - Providence Milwaukie Hospital, OR - Providence Newberg MC, OR - Providence Portland MC, OR - Providence Seaside Hospital, OR - Providence St. Vincent MC, OR - Providence Willamette Falls MC, PHCC - Home & Community Care, PHCC - Home Health, PHCC - Home Medical Equipment, PHCC - Hospice, PHCC - Infusion/Pharmacy, PHCC - PACE, PHCC - Palliative Care, PHCC - Skilled Nursing/Assisted Living, Providence, Providence Express Care, Providence Global Center, Providence Physician Enterprise, Providence Traditional Health Workers, TX - Covenant Children's Hospital, TX - Covenant Health - ACO, TX

- Covenant Health Partners, TX - Covenant Hospital Levelland, TX - Covenant Hospital Plainview, TX - Covenant Medical Center, TX - Covenant Medical Group, TX - Covenant Specialty Hospital, TX - Grace Clinic, TX - Grace Surgical Hospital, WA - Credena Health, WA - EWA Providence Medical Group, WA - Kadlec Regional Medical Center, WA - NWR Providence Medical Group, WA - PacMed, WA - Providence Centralia Hospital, WA - Providence DominiCare, WA - Providence Holy Family Hospital, WA - Providence Mt. Carmel Hospital, WA - Providence Regional MC Everett, WA - Providence Sacred Heart Med Ctr & Children's, WA - Providence St. Joseph's Hospital, WA - Providence St. Luke's Rehabilitation Medical, WA - Providence St. Mary MC, WA - Providence St. Peter Hospital, WA - SWR Providence Medical Group, WA - Swedish Medical Center, WA - Swedish Medical Group, WA - USFHP

Standards

No standards are associated with this document

Status Active PolicyStat ID 16990029

Origination	03/2020
Last Approved	11/2024
Effective	11/2024
Last Revised	11/2024
Next Review	11/2025

Owner	David Lane: Chief Compliance Officer
Policy Area	Compliance
Applicability	Providence Systemwide + PGC
Departments	Posted on Internet

PSJH-CPP-733 Nonretaliation

Executive Sponsor:	Darryl Elmouchi, MD, Chief Operations Officer
Policy Owner:	David Lane, VP, Chief Compliance Officer
Contact Person:	Karen J. Coleman, Director, Compliance Services

Scope:

This policy applies to Providence and its Affiliates[i] (collectively known as “Providence”) and its workforce (caregivers, volunteers, trainees, interns, apprentice, students), independent contractors, vendors and all other individuals working at the ministry, whether they are paid by or under the direct control of the facility); employees of affiliated organizations (collectively, “workforce members”).

☑ Yes ☐ No Is this policy applicable to Providence Global Center (PGC) caregivers?

This is a management level policy reviewed and recommended by the Policy Advisory Committee (PAC) to consider for approval by senior leadership which includes vetting by Executive Council with final approval by the President, Chief Executive Officer or appropriate delegate.

Purpose:

To establish a policy that protects workforce members from retaliation or harassment for having raised concerns about actual or potential wrongdoing or misconduct.

Definitions:

1. ***Retaliation:*** Any adverse action taken against a workforce member because the workforce member has, in good faith, reported wrongdoing or has, in good faith, cooperated in/with an investigation. Adverse actions may include actions such as scheduling changes, physical relocation, adverse evaluations, paid administrative leave, and termination. Retaliation is prohibited by law.

2. ***Workforce member*** is defined as all employees, volunteers, trainees, independent contractors, vendors, and other persons under direct control of a Providence entity, whether they are paid by Providence.

3. ***Wrongdoing*** may include, but is not limited to:
    - Illegal or fraudulent activity.
    - Financial misstatements, or accounting or auditing irregularities.
    - Conflicts of interests, or dishonest or unethical conduct.
    - Violations of the Code of Conduct.
    - Violations of applicable laws, rules, regulations, and/or policies.

4. ***Compliance Program*** is fully described in the Board approved Providence Compliance Program Description and includes the Codes of Conduct and a number of integrity and compliance policies for our family of organizations.

Policy:

Workforce members have a responsibility and duty to promptly report concerns about actual or potential wrongdoing – including violations of Providence's Compliance Program – through proper channels and are not permitted to overlook such actual or potential wrong-doing.
Providence prohibits retaliation against any workforce member for making a good-faith report of their concerns about actual or potential wrong-doing – including violations of the Providence Compliance Program. Retaliation is also prohibited against any workforce member who in good faith assists in the investigation of any reported concern. Any manager, supervisor, employee, or other workforce member who engages in retaliation or harassment is subject to discipline or other appropriate corrective action up to and including termination.

Requirements:

1. The responsibility to report and the commitment to an environment free from retaliation are communicated to workforce members through regular integrity and compliance education, their managers, and through the Providence Compliance Program.

2. Workforce members cannot exempt themselves from the consequences of wrong-doing or inadequate performance by reporting such wrong-doing or inadequate performance. However, the consequences of wrong-doing or inadequate performance may not, in any case, be more severe because a workforce member reported it on their own initiative.

3. A workforce member may file reports of incidents of retaliation or suspected retaliation either by identifying themself or anonymously. Good faith reports of retaliation or

suspected retaliation will be kept confidential to the extent possible, consistent with the need to conduct an appropriate investigation.

4. Any concerns regarding potential retaliation should be reported to the Divisional Compliance Office, Risk Department or Human Resources for investigation and resolution.

References:

Guidance from the Office of the Inspector General (OIG): At a minimum, comprehensive compliance programs should include the following: ...The adoption of procedures to protect the anonymity of complainants and to protect whistleblowers from retaliation. 63 FR 35, p. 8989
Deficit Reduction Act: Public Law 109-71
False Claims Act: 31 U.S.C. §§ 3729-3733
Compliance Program Description
Providence Code of Conduct
PSJH-CPP-711 Fraud and Abuse Prevention and Detection
PSJH-CPP-722 Code of Conduct Policy
PSJH-CPP-735 Investigations Policy
PSJH-CPP-736 Compliance Hotline Policy
PSJH-CPP-741 Disclosure Program Policy
PSJH-CPP-743 Compliance Reporting Obligations Policy
https://oig.justice.gov/hotline/whistleblower-protection

Applicability:

[i] For purposes of this policy, “Affiliates” is defined as any not-for-profit or non-profit entity that is wholly owned or controlled by Providence St. Joseph Health (PSJH), Providence Health & Services, St. Joseph Health System, Western HealthConnect, Kadlec, Covenant Health Network, Grace Health System, Providence Global Center*, NorCal HealthConnect, or is a not-for-profit or non-profit entity majority owned or controlled by PSJH or its Affiliates and bears the Providence, Swedish Health Services, St. Joseph Health, Covenant Health, Grace Health System, Kadlec, or Pacific Medical Centers names (includes Medical Groups, Home and Community Care, etc.). *Policies and/or procedures may vary for our international affiliates due to regulatory differences.

Approval Signatures

Step Description	Approver	Date
Policy Owner	David Lane: Chief Compliance Officer [CJ]	11/2024

Policy Contact	Karen Coleman: Director Compliance	11/2024

Applicability

AK - Credena Health, AK - Providence Alaska MC, AK - Providence Kodiak Island MC, AK - Providence Medical Group, AK - Providence Seward MC, AK - Providence St. Elias Specialty Hospital, AK - Providence Valdez MC, CA - Credena Health, CA - Healdsburg Hospital, CA - Petaluma Valley Hospital, CA - Physician Enterprise Northern, CA - Physician Enterprise Southern, CA - Providence Cedars-Sinai Tarzana MC, CA - Providence Holy Cross MC, CA - Providence LCM MC San Pedro, CA - Providence LCM MC Torrance, CA - Providence Mission Hospitals, CA - Providence Queen of the Valley Medical Center, CA - Providence Redwood Memorial Hospital, CA - Providence Saint John's Health Center, CA - Providence Saint Joseph MC, Burbank, CA - Providence Santa Rosa Memorial Hospital, CA - Providence St. Joseph Hospital - Eureka, CA - Providence St. Joseph Hospital Orange, CA - Providence St. Jude Medical Center, CA - Providence St. Mary Medical Ctr Apple Valley, MT - Credena Health, MT - Providence St. Joseph MC, Polson, MT - St. Patrick Hospital, NM - Covenant Hobbs Hospital, OR - Credena Health, OR - Providence Ctr for Medically Fragile Children, OR - Providence Health Oregon Labs, OR - Providence Hood River Memorial Hospital, OR - Providence Medford MC, OR - Providence Medical Group, OR - Providence Milwaukie Hospital, OR - Providence Newberg MC, OR - Providence Portland MC, OR - Providence Seaside Hospital, OR - Providence St. Vincent MC, OR - Providence Willamette Falls MC, PHCC - Home & Community Care, PHCC - Home Health, PHCC - Home Medical Equipment, PHCC - Hospice, PHCC - Infusion/Pharmacy, PHCC - PACE, PHCC - Palliative Care, PHCC - Skilled Nursing/Assisted Living, Providence, Providence Express Care, Providence Global Center, Providence Physician Enterprise, Providence Traditional Health Workers, TX - Covenant Children's Hospital, TX - Covenant Health - ACO, TX - Covenant Health Partners, TX - Covenant Hospital Levelland, TX - Covenant Hospital Plainview, TX - Covenant Medical Center, TX - Covenant Medical Group, TX - Covenant Specialty Hospital, TX - Grace Clinic, TX - Grace Surgical Hospital, WA - Credena Health, WA - EWA Providence Medical Group, WA - Kadlec Regional Medical Center, WA - NWR Providence Medical Group, WA - PacMed, WA - Providence Centralia Hospital, WA - Providence DominiCare, WA - Providence Holy Family Hospital, WA - Providence Mt. Carmel Hospital, WA - Providence Regional MC Everett, WA - Providence Sacred Heart Med Ctr & Children's, WA - Providence St. Joseph's Hospital, WA - Providence St. Luke's Rehabilitation Medical, WA - Providence St. Mary MC, WA - Providence St. Peter Hospital, WA - SWR Providence Medical Group, WA - Swedish Medical Center, WA - Swedish Medical Group, WA - USFHP

Standards

No standards are associated with this document

Status Active PolicyStat ID 15900996

Origination	05/2021	Owner	Michael Ratliff: AVP IS Security Engineering
Last Approved	05/2024	Policy Area	Cybersecurity
Effective	05/2024	Applicability	Providence Systemwide + PGC
Last Revised	05/2024		
Next Review	05/2029		

PSJH-CYBR-950.08 Acceptable Use Standard - Corresponds to: PSJH-CYBR-950 Information Security Management Policy

Purpose:

This standard is a mandatory course of action or rules that give the formal policy support and direction. It establishes Providence requirements for acceptable use of computer equipment and resources.

Definitions:

Confidential Information is any information, regardless of format, about patients, employees, students, residents, or business operations that Providence deems should not be available without specific authorization. Loss or inappropriate access to this kind of data could harm patients, Providence reputation and ability to do business. Confidential information includes but is not limited to PHI, ePHI, PII, card holder data (PCI), employee information, financial information and any other information that is intended for limited internal use by Providence.

Local Storage: Data storage that is directly attached to a computer or device.

Users: Workforce members and other individuals who require access to Providence data systems, process, devices and networks in order to provide a service or functions necessary for the conduct of business with or for Providence. Determination of access permissions is based on business need and security requirements. Users are authorized through an individual user agreement, employment contract, or through a contract between Providence and a third party employer.

For the definition of terms not specifically defined above, please refer to PSJH-CPP-850.05, Privacy and Security Glossary.

Policy Linkage:

System Policy: PSJH-CYBR-950, Information Security Management Policy.

Standard:

This technical standard and/or detailed procedure is an extension of the policy linked above. For scope and applicability of this standard, refer to the parent policy. The standard is in place to protect the confidentiality, integrity and availability of Providence information and information systems. Inappropriate use exposes Providence to risks including malware attacks, compromise of network systems and services, and litigation.

Requirements:

A. **General requirements for the use of Providence information and information systems**

1. All authorized Providence workforce members have a responsibility to protect Providence information and information systems. Users must only access Providence information and information systems for which they are authorized and only access such information using approved devices and services. Misuse of Providence information and information systems may put the organization, data, and patients at risk.
2. Personal use of Providence resources is a limited privilege. Limited personal use of information systems is permitted with the following restrictions: usage must be reasonable, ethical and legal and usage must not interfere with any workforce members' responsibilities or productivity. Providence Information Services may limit the quantity and/or type of personal-use files stored on information systems or networks.
3. Prior to accessing Providence information and information systems users are required to acknowledge and agree to follow the Acceptable Use Standard. Users holding an employment contract or who work through a third-party contract between Providence and the user's third- party employer are required to acknowledge and agree to follow an appropriate acceptable use agreement maintained by Contracting and Procurement. Failure to acknowledge this agreement or violation of this agreement may result in denial of access to Providence information and information systems.
4. Users connecting an approved mobile device to Providence information systems must follow the requirements in the PSJH-CYBR-951.01, Information Technology Asset Management standard. The mobile device must meet all the required security controls. This applies to all devices whether personally owned or issued by Providence.
5. Providence reserves the right to monitor all use of Providence information systems and all access to Providence electronic data. Users of Providence information systems have no expectation of privacy with regards to content or use of electronic communications or data within any Providence information system.

6. Providence paper documents, computers, and mobile storage and computing devices must be protected from loss, theft, unauthorized use, disclosure, modification, or destruction. They must be physically secured when taken off site.
7. All authorized users must take all reasonable steps to protect the privacy and security of confidential patient and confidential business information. In order to minimize the potential for loss and disclosure, confidential patient information, whether in paper or electronic format, must always be in the possession of the Providence employee or agent, or in a secure location.
8. All users are required to promptly report the loss, theft, unauthorized use, unauthorized disclosure, unauthorized modification or unauthorized destruction of paper documents, electronic data, computers, or mobile storage and computing devices by notifying the Information Service Desk.
9. All authorized users are required to cooperate with Providence investigation or remediation efforts related to information security incidents.
10. All authorized users must follow the requirements in this document and all other requirements in Providence's policies and standards. Any violation of these requirements may result in corrective action up to and including termination of employment or termination of contractual arrangement(s) with Providence. Violations may subject individuals to civil and/or criminal penalties.
11. Nothing in this policy is intended to restrict employees from discussion, transmission or disclosure of wages, hours and working conditions in accordance with applicable federal and state laws.

B. **Terms of Acceptable Use:** Acceptable use of Providence information and information systems by authorized users is generally described below:

1. **User Access**

    a. Users are only permitted to use their own Providence-assigned IDs and must not use the credentials that were assigned to other users.

    b. Users are accountable to protect the confidentiality their unique IDs and passwords.

    c. Users must not employ the same password used for Providence accounts to access other non-Providence accounts (e.g. personal ISP account, website accounts, etc.).

    d. Users are encouraged not to use Providence provided identification and authentication information (e.g., email address, account names) for non-Providence work or for creating accounts on external sites/applications.

    e. Users may not share their passwords with anyone.

    f. Passwords must follow Providence password requirements.

    g. Users must not print or store passwords insecurely. Passwords must not be written down.

    h. Users must inform the Information Services Service Desk and must change their password, and other credentials, if they believe that their passwords or other credentials are compromised.

i. Users are not allowed to access Providence information or information systems for which they have not been authorized.

j. The use and handling of mobile storage and computing devices is restricted to those individuals who are authorized to access these devices.

k. Users accessing confidential information (including Protected Health Information) are only authorized to access the minimum information necessary to do their jobs.

l. When accessing Providence confidential information from an off-site location, users must use reasonable safeguards to ensure that the work session cannot be viewed or accessed by unauthorized individuals.

m. Users must secure all applications (log out/lock) when leaving a workstation unattended or accessible to unauthorized individuals (e.g., patients, visitors).

n. Users may only use approved remote access services meeting Providence security requirements and approved by Information Services and Cybersecurity.

o. Authorized users may not allow any unauthorized user to access Providence information systems or data.

p. Shared workstations (e.g., "auto-login" workstations) must be configured with a unique network identification that is automatically logged on to the Providence network. Access to any confidential information from such shared workstation must require individual user authentication.

q. Users must not store confidential information locally on shared workstations.

2. **Computing Devices and Software**

a. Workforce member personal devices are not authorized to connect to the Providence corporate network except where network access controls, or similar technologies, are in place to isolate personal devices from Providence production systems, data, and medical devices. Any such personal device must also have:

   I. A current and supported operating system, current security patches, and must not be jailbroken.

   II. Additionally, personal computers (PC, Mac, Linux, etc.) connecting to the network must have current operating systems, current security patches, and must have a current and supported anti-malware software installed and effectively operating.

b. If network isolation controls are not in place, or if caregiver personal devices do not meet the requirements listed in section above, then these devices must use cellular networks or the Providence Guest network instead of the production network.

c. Workforce member devices connected to the Providence network are subjected to removal if they represent a risk to Providence systems or data, or other reasons to be determined by Cybersecurity or Information Services.

d. The use of all electronic storage media/portable storage devices must follow Providence standard PSJH-CYBR-951.01, Information Technology Asset Management.

e. Only software and applications authorized by Information Services and have passed a Cybersecurity review may be installed on a Providence computing system or a Providence mobile computing device. Refer to Providence standard PSJH-CYBR-950.05, Vendor Security Risk Management.

f. An automobile is not considered a secure location and should not be used to store confidential information, papers or mobile computing or storage devices. A mobile computing device should never be left unattended in an automobile. However, in some circumstances it may be preferable for the user to leave an appropriately secured tablet or laptop computer in a vehicle rather than removing it from the vehicle. Examples of such circumstances include:

    i. The vehicle will only be unoccupied for a few minutes in a well-observed location.

    ii. Removing the laptop or tablet from the vehicle will expose the device to more likelihood of loss or theft due to a crowded public venue.

    iii. It is infeasible to take the laptop or tablet due to physical constraints. ***In such circumstances, a Providence laptop or tablet may be left in an automobile as long as the following conditions are met:***

        a. The device must be stored out out-of-sight (e.g., under a seat or in the trunk).

        b. The vehicle must be locked.

g. Transportation of Providence computing devices (e.g. laptops, tablets, smartphones, storage devices) outside of the United States requires approval, and is subject to the following restrictions:

    i. Under no circumstances must a Providence computing device be transported to a country subject to a United States State Department Travel Warning: http://travel.state.gov/content/passports/en/alertswarnings.html

    ii. Providence does not allow permanent remote working outside of the United States. Providence workforce members may seek temporary remote work outside of the United States provided that the following conditions are met: Providence computing devices will only be transported to countries that are not under a State Department Travel warning, the caregiver obtains written approvals from System Director (or above), Division or Line of Business Chief Human Resources Officer, Chief Risk Officer, and Senior Corporate Counsel of the Department of Legal Affairs (DLA). The written approvals must be obtained prior to traveling. Each such request will be evaluated on a case-by-case basis.

iii. Any Providence computing device authorized for transport outside the United States is required to meet the following conditions:

a. Transport of the device to the foreign country must be required for conducting Providence business.

b. Providence computing devices must be encrypted.

c. Providence authorized Virtual Private Network (VPN) connections and monitoring tools shall be turned on at all times.

d. Any non-required confidential information must be removed from the device prior to travel abroad.

e. Any inspections, tampering or loss of custody of the device must be immediately reported to the Enterprise Information Services Service Desk.

f. The device must not be packed in checked baggage during travel.

h. Papers containing confidential information and mobile storage and computing devices must not be checked with baggage on commercial transportation (e.g., airline, train).

i. Under no circumstances are workforce members to use mobile computing devices, mobile phones or pagers while operating a motor vehicle unless such use is hands- free, meets applicable laws and regulations and does not interfere with the safe operation of the vehicle.

j. Providence computers must comply with a standard desktop build managed by Information Services. This includes but is not limited to the installation of current security patches/updates, current malware protection software, endpoint detection and response (EDR) client, client firewall and firewall configuration, and password protection.

k. Users may not modify or attempt to remove or disable Providence standard software and hardware security controls and system configurations of Providence computers except as authorized in writing by Information Services.

l. Computing devices must connect with Providence infrastructure (either locally or remotely via VPN) at least monthly in order to receive automated maintenance and inventory services.

3. **Confidential Information**
    a. When electronic confidential information is stored, transported or transmitted outside Providence facilities it must be encrypted.
    b. Confidential information may be used, accessed or disclosed only to those who have a need to know. Only the minimal necessary amount of confidential information must be used, accessed or disclosed.
    c. Any portable storage or computing device containing Providence confidential information must be encrypted, and password protected.
    d. Confidential information must deleted or removed from the Providence information systems in accordance with the PSJH-CPP-715 Records Retention and Disposal policy.
    e. Providence information classified as confidential or internal use must not be printed at off- site locations without the appropriate level of Providence management approval.
    f. All use of Providence confidential information off site must follow Providence standard PSJH-CYBR-951.01 Information Technology Asset Management relating to device and media handling, storage and transport.
    g. Paper documents and storage and computing devices containing confidential or internal use information must be secured from unauthorized access or use while awaiting destruction and must be destroyed in accordance with Providence standard PSJH-CYBR-965.01 Data Handling and Destruction.
    h. Confidential information must not be stored on personal computing devices, personal mobile devices, personal cloud storage environments (e.g., personal OneDrive, Google Drive, Dropbox, Box.com, etc.), or on personal mass media storage devices (e.g., USB drives, external hard drives, flash storage cards., etc.). Personal phones or tablets enrolled in Providence's Bring Your Own Device (BYOD) program may store Confidential Information in applications enrolled in BYOD, like Microsoft Office 365 programs administered by Providence or Providence managed Epic applications.

4. **Confidential Patient Information:** Authorized users providing patient care in a home setting must secure all confidential patient information by meeting the following requirements:
    a. Take only the minimum necessary information for the care of current patients located off site.
    b. Once a patient is no longer under the care of Providence, their confidential information must be deleted from mobile devices and all associated paper documents must be disposed of in accordance with Providence standard PSJH-CYBR-965.01, Data Handling and Destruction.
    c. When involved in patient care in a home setting, confidential patient

information must be protected from unauthorized access.

d. Authorization by a supervisor is required for an employee to store confidential patient information in their home. Authorization is to be based on particular circumstances or a particular job description.

e. Patient confidential information (ePHI) stored temporarily at home must be kept in a secure location such as a locked drawer, cupboard or office.

5. **Internet Use**

   a. All use of social media (e.g., social networking) must be in accordance with the Providence Social Media Policy, available on the Caregiver Service Portal.

   b. Providence blocks categories of inappropriate Internet sites because of information security risks or as requested by leadership. Purposeful attempts to access blocked sites are a violation of this policy.

   c. Providence blocks Internet cloud service sites for sharing documents and data. Internet website services or cloud services refer to any resource that is provided over the Internet. Examples of cloud services include, but are not limited to:

      i. Any site on the Internet asking to create a user name/password and login.

      ii. Any site where entering patient information through a website form. This includes sites set up by medical device manufactures and medical software companies.

      iii. Document sharing or note taking sites such as Dropbox, Google docs, and Evernote.

      iv. Any Non-Providence system that stores Providence data must be approved by Information Security and have an appropriate contract and/or Business Associate Agreement.

      v. Workforce members are subject to Internet filtering and must use approved methods to access the Internet from Providence facilities.

      vi. Authorized users are responsible to ensure that Internet content accessed via Providence information systems is appropriate for the workplace. Internet access may be limited or disabled at the discretion of Providence.

6. **Intranet and Extranet Use**

   a. Providence's SharePoint Online and other collaborative tools are intended for Providence business purposes only.

   b. External parties are not allowed to connect to the Providence SharePoint Online environment unless it is with express permission of the appropriate level of Providence management. Permission must be granted via a formal agreement/contract to address specific business needs.

c. Confidential information posted to Providence's SharePoint Online environment is subject to the requirements of the Confidentiality Policy (available on the Caregiver Service Portal).

d. Access to the Providence SharePoint online environment must only be provided to address particular business needs of external parties and Providence.

7. **Electronic Communication**

a. Providence regularly monitors electronic communications on its systems including Providence e-mail and instant messaging communications. Sending confidential information through Internet instant messaging is prohibited.

b. Providence workforce members are not permitted to use third-party e-mail providers (e.g., personal e-mail accounts) to conduct Providence business.

c. Users must ensure information contained in all postings, e-mail messages, or any other form of electronic transmission is accurate, appropriate, ethical, truthful, and lawful.

d. Users who have been delegated access to another person's electronic information e.g., e-mail, and calendar, must only access the information when needed.

e. Users may only subscribe to list server discussion groups that are specifically job-related. Legitimate list server subscribers are expected to maintain Providence confidentiality guidelines in all list server discussion correspondence. When participating in list server discussion groups the following disclaimer must be attached to the subscriber's post*: The views and opinions expressed do not necessarily state or reflect those of Providence St. Joseph Health and its Affiliates. Providence assumes no liability or responsibility for the accuracy, completeness, or usefulness of the information communicated*.

f. Workforce members must be aware that Cybersecurity and Information Services can retrieve or view electronic communications including e-mail regardless of whether the sender and receiver have deleted their copies.

g. User e-mail accounts will be deleted upon notification of termination of employment or contract with Providence. Management may request transfer of mailbox contents prior to termination. Providence may retain mailbox contents as needed.

h. E-mail is a communication tool and is not to be used as a storage mechanism for information. Information subject to specific retention requirements should be stored separately in a suitable electronic or paper system.

i. To prevent viruses, malware and other disruptions to Providence information systems, users must avoid opening suspicious e-mails and accessing suspicious or inappropriate websites.

8. **Personally-Owned Devices**

    a. Personally-owned devices must meet Providence security requirements and may not connect to Providence information systems or store Providence confidential information unless authorized by Information Services.

    b. Workforce members will be authorized to connect to Providence systems or networks with an approved smartphone, tablet/i-Pad device only upon enrolling the device through Providence's standard online enrollment process.

    c. Personally-owned devices connecting to the Providence internal network must have current anti-virus installed, an updated operating system with current patches and current application patches.

    d. Personally-owned devices may only be used to access Providence confidential information through approved access methods, but cannot be used to store Providence information.

    e. Any approved smartphone must support the following security controls before connection to Providence networks is allowed:

        i. Providence device administrators must have the ability to apply or configure appropriate device security controls.

        ii. A password, PIN, or biometric authentication (fingerprint or Facial ID) must be enforced on the device.

        iii. Device passwords or PIN must have a minimum length of 6 characters.

        iv. Applications on the device that store, process, or transmit Providence confidential information must be part of Providence's managed suite of applications.

        v. For the devices where automatic lock is configurable, those devices must be configured to password lock after a maximum of 10 minutes of inactivity.

        vi. Providence information classified as confidential or internal use must be encrypted.

        vii. Providence information should not be stored on personal devices except via applications that are enrolled in Application Protection Policies.

    f. Providence specifically forbids the transfer of confidential information to user-owned storage or computing devices.

9. **Prohibited Usage:** Prohibited communication activities include but are not limited to:

    a. Creating or distributing discriminatory, harassing or other threatening messages or images. Caregivers encountering or receiving this kind of material must immediately report the incident to their supervisor.

b. Creation, storage or distribution of unacceptable content including, but not limited to, sexual comments or images, pornography, racial slurs, hate materials, or any other comments or images that could reasonably offend someone on the basis of race, age, sex, religious or political beliefs, national origin, disability, sexual orientation, or any other characteristic protected by law.

c. Sending chain letters, broadcasting messages unnecessarily, sending messages repeatedly, and excessive or frivolous use of electronic communication technologies.

d. Communicating messages that denigrate, defame, or slander the products or services of Providence or other entities or individuals.

e. E-mailing or otherwise sending confidential information to a personal e-mail account or Internet storage service.

f. Violation of the copyright or trademark law.

g. Violation of confidentiality or non-disclosure agreements.

h. Installation of software not authorized by Information Services.

i. Violation of licensing agreements.

j. Gambling, unlawful activity or any activity inconsistent with Providence core values.

k. Representing personal views as those of Providence, including unauthorized use of the official logo.

l. Attempting to gain unauthorized access to a computer system of another organization or person.

m. Impersonating another person when sending email messages.

n. Deliberately jeopardizing the security of any Providence information system.

o. Engaging in any conduct that is contrary to, or inconsistent with, the mission and values of Providence.

10. **Recording Devices in the Workplace**

a. Those working on behalf of Providence must not record, monitor, or otherwise intercept the communications or activity of anyone through the use of any electronic, mechanical, or other recording devices except for official business use.

b. Camera or mobile devices that have built in recording capability may be used for personal communication/assistance in appropriate areas. The recording capability of such devices must not be used in business/clinical areas without prior authorization.

Regulatory and Contractual Requirements:

The security of confidential information (including electronic Protected Health Information (ePHI)) is of particular importance. Violations of provisions of HIPAA can damage Providence's reputation as a responsible leader in healthcare and result in employee sanctions (up to, and including, termination of employment), revocation of professional licensure/accreditation, significant civil monetary and/or criminal penalties. This standard applies to Providence ePHI as well as, more broadly, to all Providence information. Any references to particular regulatory or contractual requirements (e.g., HIPAA, FDA regulations, state laws, PCI-DSS) are intentionally minimized so as not to indicate that this policy is exclusive to specific categories of information (e.g., ePHI, PII, student records, employee records, genetic information, trade secret information).

Non-Compliance:

All Providence workforce members shall understand their roles and responsibilities for protecting Providence information and physical assets. Failure to comply with the Cybersecurity Policy may result in corrective actions up to and including termination of employment for employees or termination of contract for contractors, partners, consultants, and other entities. Violations may subject individuals (and the organization) to civil and/or criminal penalties.

References:

See the Confidentiality Policy and the Use of Cell Phones and Personal Devices Policy, available on the Caregiver Services Portal

PSJH-CPP-715 Records Retention and Disposal

PSJH-CYBR-950.04 Vendor Security Risk Management

PSHJ-CYBR-951.01 Information System Acquisition, Development and Maintenance

PSJH-CYBR-965.01 Data Handling and Destruction

This document is classified Providence Confidential. Do not redistribute without the approval of Compliance and Privacy Services / Information Security Services.

Approval Signatures

Step Description	Approver	Date
PSJH President/CEO	Cynthia Johnston: Principal Compliance Consultant	05/2024
PSJH Executive Council	Cynthia Johnston: Principal Compliance Consultant	05/2024
PSJH Policy Advisory Committee	Cynthia Johnston: Principal Compliance Consultant	05/2024

Applicability

AK - Credena Health, AK - Providence Alaska MC, AK - Providence Kodiak Island MC, AK - Providence Medical Group, AK - Providence Seward MC, AK - Providence St. Elias Specialty Hospital, AK - Providence Valdez MC, CA - Credena Health, CA - Healdsburg Hospital, CA - Petaluma Valley Hospital, CA - Physician Enterprise Northern, CA - Physician Enterprise Southern, CA - Providence Cedars-Sinai Tarzana MC, CA - Providence Holy Cross MC, CA - Providence LCM MC San Pedro, CA - Providence LCM MC Torrance, CA - Providence Mission Hospitals, CA - Providence Queen of the Valley Medical Center, CA - Providence Redwood Memorial Hospital, CA - Providence Saint John's Health Center, CA - Providence Saint Joseph MC, Burbank, CA - Providence Santa Rosa Memorial Hospital, CA - Providence St. Joseph Hospital - Eureka, CA - Providence St. Joseph Hospital Orange, CA - Providence St. Jude Medical Center, CA - Providence St. Mary Medical Ctr Apple Valley, MT - Credena Health, MT - Providence St. Joseph MC, Polson, MT - St. Patrick Hospital, NM - Covenant Hobbs Hospital, OR - Credena Health, OR - Providence Ctr for Medically Fragile Children, OR - Providence Health Oregon Labs, OR - Providence Hood River Memorial Hospital, OR - Providence Medford MC, OR - Providence Medical Group, OR - Providence Milwaukie Hospital, OR - Providence Newberg MC, OR - Providence Portland MC, OR - Providence Seaside Hospital, OR - Providence St. Vincent MC, OR - Providence Willamette Falls MC, PHCC - Home & Community Care, PHCC - Home Health, PHCC - Home Medical Equipment, PHCC - Hospice, PHCC - Infusion/Pharmacy, PHCC - PACE, PHCC - Palliative Care, PHCC - Skilled Nursing/Assisted Living, Providence, Providence Express Care, Providence Global Center, Providence Physician Enterprise, Providence Traditional Health Workers, TX - Covenant Children's Hospital, TX - Covenant Health - ACO, TX - Covenant Health Partners, TX - Covenant Hospital Levelland, TX - Covenant Hospital Plainview, TX - Covenant Medical Center, TX - Covenant Medical Group, TX - Covenant Specialty Hospital, TX - Grace Clinic, TX - Grace Surgical Hospital, WA - Credena Health, WA - EWA Providence Medical Group, WA - Kadlec Regional Medical Center, WA - NWR Providence Medical Group, WA - PacMed, WA - Providence Centralia Hospital, WA - Providence DominiCare, WA - Providence Holy Family Hospital, WA - Providence Mt. Carmel Hospital, WA - Providence Regional MC Everett, WA - Providence Sacred Heart Med Ctr & Children's, WA - Providence St. Joseph's Hospital, WA - Providence St. Luke's Rehabilitation Medical, WA - Providence St. Mary MC, WA - Providence St. Peter Hospital, WA - SWR Providence Medical Group, WA - Swedish Medical Center, WA - Swedish Medical Group, WA - USFHP

Standards

No standards are associated with this document

Status Active PolicyStat ID 15579659

Origination	05/2021	Owner	Michael Ratliff: AVP IS Security Engineering
Last Approved	04/2024	Policy Area	Cybersecurity
Effective	04/2024	Applicability	Providence Systemwide + PGC
Last Revised	04/2024		
Next Review	04/2029		

PSJH-CYBR-962.01 Security Risk Management Standard - Corresponding Policy: PSJH-CYBR-962 Information Security Management Policy

Purpose:

This standard is a mandatory course of action or rules that give the formal policy support and direction. This document contains the minimum specifications for Providence's formal Security Risk Management Program to ensure confidentiality, integrity and availability of all Providence information systems.

Definitions:

For the definition of terms not specifically defined below, please refer to the PSJH-CPP-850.05 Privacy and Security Glossary.

Mitigation: The elimination or reduction of the frequency, magnitude, or severity of exposure to risks, or minimization of the potential impact of a threat.

Risk: A probability or threat of damage, injury, liability, loss, or any other negative consequence that is caused by external or internal vulnerabilities, and that may be avoided through preemptive action.

Risk Levels: Categorization used to classify the severity and likelihood of a risk within the context of Risk Management. Refer to the Assessment Scale -Level of Risk table below (Table 1.1 and 1.2)

Risk owner: The Providence Executive responsible for the business process that presents the risk and authorized to sign-off on the monetary and/or reputational impact should the risk be realized.

Third party: Someone who may be directly or indirectly processing information or conducting business on behalf of or in partnership with Providence but is not acting in the capacity of a Providence workforce member.

Integrated Controls Framework (ICF): The collective body of legal, regulatory, industry standards (e.g., HIPAA, PCI DSS, NIST 800-53) employed by Providence to secure and protect the confidentiality, integrity and availability of the information used, transmitted and/or stored by Providence.

Threat: Any circumstance or event with the potential to adversely impact organizational operations (including but not limited to mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Vulnerability: A weakness in a system, application, or network that is subject to exploitation or misuse.

Impact: The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.

Policy Linkage:

System Policy PSJH-CYBR-962, Security Risk Management Policy.

Standard:

This technical standard and/or detailed procedure is an extension of the policy linked above. For scope and applicability of this standard, refer to the parent policy.

Requirements:

A. 1. **Information Security Risk Management Program (ISRMP):**

a. Providence shall establish a dedicated team with assigned responsibilities to implement and operate security risk management processes across the enterprise.

b. Providence shall establish an Information Security Risk Management Program (ISRMP) to define the scope, objectives and high-level requirements to identify, assess, prioritize, mitigate, and monitor security risks to Providence, such that the identified security risks are maintained at an acceptable level. At a minimum, the ISRMP shall:

1. Approve, communicate, and document security risk appetite or risk acceptance criteria.

2. Establish a security categorization method for information systems based upon the security impact to Providence resulting from a loss of confidentiality, integrity, or availability of information.
3. Conduct security risk assessments and identify security risk treatment actions via a security risk management plan.
4. Track and manage security risks and associated security risk treatment actions using a central risk register.
5. Identify and monitor Key Risk Indicators (KRI) for residual security risk.
6. Periodically review the outcomes of prior security risk assessments.
7. Use all-source intelligence, i.e., publicly available or open-source information, measurement and signature intelligence, human intelligence, signals intelligence, and imagery intelligence to analyze the risk of vulnerabilities (both intentional and unintentional) from development, manufacturing, and delivery processes, people, and the environment. Providence may develop agreements to share all-source intelligence information or resulting decisions with other organizations, as appropriate.
8. Disseminate risk assessment results to relevant stakeholders (e.g. system owners, risk owners, risk management leadership).
9. Review and approve accepted risks periodically or at the end of defined expiry period.

c. Providence shall establish a process for conducting targeted risk analysis for applicable standards or regulatory requirements (e.g. HIPAA, PCI-DSS). The process shall clearly define scope, objectives, approach, and frequency of the targeted risk analysis.

d. Providence shall conduct targeted risk analysis leveraging the established process and methodology at the frequency defined by applicable standards or regulatory requirements (e.g., HIPAA, PCI-DSS).

e. Results of the targeted risk analysis shall be documented, maintained, and approved by designated authorities.

f. Targeted risk analysis results shall be reviewed at least once every 12 months to determine the validity of the results or the need for a new targeted risk analysis.

g. A criticality analysis shall be performed during identified decision-points in the System Development Life Cycle (SDLC) in order to identify mission/ business critical system components.

2. **Security Risk Appetite Statement or Acceptance Criteria:**

a. Cybersecurity shall define the risk appetite and acceptance criteria to provide the threshold and type of risks acceptable to Providence. This should further guide the selection of appropriate risk treatment strategies for the identified risks.

3. **Security Categorization:**

    a. Business or Asset owners shall categorize and document the categorization of their information systems based on the potential impact to Providence caused by certain events that jeopardize the confidentiality, integrity, and availability of the information and information systems.

    b. Each information type within an information system should be categorized based upon defined criticality. The highest security mark for each information type determines the overall security categorization for the information system.

    c. Security categories shall be used to determine the baseline security controls for information systems, which should be further aligned based on the risk assessment process.

    d. Authorizing/authorized official or their designated representatives shall review and approve the security categorization of information and information systems.

4. **Security Risk Assessment Triggers:**

    a. Security risk assessments shall be initiated due to the following:

        i. Mergers and Acquisitions.

        ii. New technical solutions/applications/software that will be utilized to conduct Providence business regardless of whether they are in-house built or provided by new vendors.

        iii. Major infrastructure changes or upgrades to existing information systems.

        iv. Periodic risk assessment of existing information systems.

        v. New business contract establishment or renewal

5. **Technical and Non-technical Security Assessments:**

    a. Cybersecurity shall perform security assessments to determine whether security controls consistent with Providence Security Policies and Standards are in place.

    b. Cybersecurity shall implement technical mechanisms to perform vulnerability scanning at regular intervals, or when new vulnerabilities potentially affecting information systems are identified and reported per PSJH-CYBR-950.05 Patch and Vulnerability Management Standard for details regarding vulnerability scanning process.

Table 1.1: ASSESSMENT SCALE - LEVEL OF RISK (COMBINATION OF LIKELIHOOD AND IMPACT)

Likelihood (Threat Event Occurs and Results is Adverse Impact)	Very Low Impact	Low Impact	Moderate Impact	High Impact	Very High Impact
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

Table 1.2: ASSESSMENT SCALE-LEVEL OF RISK

Qualitative Values	Semi-Quantitative Values	Semi-Quantitative Values	Description
Very High	96-100	10	**Very high risk** means that a threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation
High	80-95	8	**High risk** means that a threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Moderate	21-79	5	**Moderate risk** means that a threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Low	5-20	2	**Low risk** means that a threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Very Low	0-4	0	**Very low risk** means that a threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.

Reference from NIST Special Publication 800-30r1, Guide for Conducting Risk Assessments

Regulatory and Contractual Requirements:

The security of confidential information (including electronic Protected Health Information (ePHI)) is of particular importance. Violations of provisions of HIPAA can damage Providence's reputation as a responsible leader in healthcare and result in employee sanctions (up to, and including, termination of employment), revocation of professional licensure/accreditation, significant civil monetary and/or criminal penalties. This standard applies to Providence ePHI as well as, more broadly, to all Providence information. Any references to particular regulatory or contractual requirements (e.g., HIPAA, FDA regulations, state laws, PCI-DSS) are intentionally minimized so as not to indicate that this policy is exclusive to specific categories of information (e.g., ePHI, PII, student records, employee records, genetic information, trade secret information).

Non-Compliance:

All Providence workforce members shall understand their roles and responsibilities for protecting Providence information and physical assets. Failure to comply with the Cybersecurity Policy may result in disciplinary actions up to and including termination of employment for employees or termination of contract(s) for contractors, partners, consultants, and other entities. Violations may subject individuals (and the organization) to civil and/or criminal penalties.

References:

NIST 800-60: Guide for Mapping Types of Information and Information Systems to Security Categories

PSJH-CYBR-950 Information Security Management Policy

PSJH-CYBR-950.02 Security Compliance Standard

PSJH-CYBR-950.03 Security Assessment and Authorization Standard

PSJH-CYBR-950.05 Patch and Vulnerability Management Standard

PSJH-CYBR-950.06 Security Exception Processing Standard

PSJH-CYBR-ICFv2 Integrated Controls Framework (ICF)

PSJH-CPP-715 Records Retention & Disposal Policy

Approval Signatures

Step Description	Approver	Date

PSJH President/CEO	Cynthia Johnston: Principal Compliance Consultant	04/2024
PSJH Executive Council	Cynthia Johnston: Principal Compliance Consultant	04/2024
PSJH Policy Advisory Committee	Cynthia Johnston: Principal Compliance Consultant	04/2024

Applicability

AK - Credena Health, AK - Providence Alaska MC, AK - Providence Kodiak Island MC, AK - Providence Medical Group, AK - Providence Seward MC, AK - Providence St. Elias Specialty Hospital, AK - Providence Valdez MC, CA - Credena Health, CA - Healdsburg Hospital, CA - Petaluma Valley Hospital, CA - Physician Enterprise Northern, CA - Physician Enterprise Southern, CA - Providence Cedars-Sinai Tarzana MC, CA - Providence Holy Cross MC, CA - Providence LCM MC San Pedro, CA - Providence LCM MC Torrance, CA - Providence Mission Hospitals, CA - Providence Queen of the Valley Medical Center, CA - Providence Redwood Memorial Hospital, CA - Providence Saint John's Health Center, CA - Providence Saint Joseph MC, Burbank, CA - Providence Santa Rosa Memorial Hospital, CA - Providence St. Joseph Hospital - Eureka, CA - Providence St. Joseph Hospital Orange, CA - Providence St. Jude Medical Center, CA - Providence St. Mary Medical Ctr Apple Valley, MT - Credena Health, MT - Providence St. Joseph MC, Polson, MT - St. Patrick Hospital, NM - Covenant Hobbs Hospital, OR - Credena Health, OR - Providence Ctr for Medically Fragile Children, OR - Providence Health Oregon Labs, OR - Providence Hood River Memorial Hospital, OR - Providence Medford MC, OR - Providence Medical Group, OR - Providence Milwaukie Hospital, OR - Providence Newberg MC, OR - Providence Portland MC, OR - Providence Seaside Hospital, OR - Providence St. Vincent MC, OR - Providence Willamette Falls MC, PHCC - Home & Community Care, PHCC - Home Health, PHCC - Home Medical Equipment, PHCC - Hospice, PHCC - Infusion/Pharmacy, PHCC - PACE, PHCC - Palliative Care, PHCC - Skilled Nursing/Assisted Living, Providence, Providence Express Care, Providence Global Center, Providence Physician Enterprise, Providence Traditional Health Workers, TX - Covenant Children's Hospital, TX - Covenant Health - ACO, TX - Covenant Health Partners, TX - Covenant Hospital Levelland, TX - Covenant Hospital Plainview, TX - Covenant Medical Center, TX - Covenant Medical Group, TX - Covenant Specialty Hospital, TX - Grace Clinic, TX - Grace Surgical Hospital, WA - Credena Health, WA - EWA Providence Medical Group, WA - Kadlec Regional Medical Center, WA - NWR Providence Medical Group, WA - PacMed, WA - Providence Centralia Hospital, WA - Providence DominiCare, WA - Providence Holy Family Hospital, WA - Providence Mt. Carmel Hospital, WA - Providence Regional MC Everett, WA - Providence Sacred Heart Med Ctr & Children's, WA - Providence St. Joseph's Hospital, WA - Providence St. Luke's Rehabilitation Medical, WA - Providence St. Mary MC, WA - Providence St. Peter Hospital, WA - SWR Providence Medical Group, WA - Swedish Medical Center, WA - Swedish Medical Group, WA - USFHP

Standards

No standards are associated with this document

Status Active PolicyStat ID 16989997

Origination	01/2010	Owner	David Lane: Chief Compliance Officer
Last Approved	11/2024	Policy Area	Compliance
Effective	11/2024	Applicability	Providence Systemwide + PGC
Last Revised	11/2024		
Next Review	11/2025		

PSJH-CPP-700 Compliance Program Policy

Executive Sponsor:	Erik Wexler, President/CEO
Policy Owner:	David Lane, VP, Chief Compliance Officer
Contact Person:	Karen Coleman, Director, Compliance Services

Scope:

This policy applies to Providence and its affiliates[1] (collectively known as "Providence") and their caregivers (employees); employees of our affiliated organizations, professional staff, volunteers and others who are in the direct control of the organization; and members of the Providence System Board; Community Boards; and Foundation Boards, trustees (collectively referred to as workforce members).

☑ Yes ☐ No Is this policy applicable to Providence Global Center (PGC) caregivers?

This is a governance level policy, vetted by Executive Council with a recommendation for approval by the Providence Board and signed by the appropriate delegate.

Purpose:

This policy supports the Compliance Program Description and provides the plan and framework for our organization to maintain an effective Compliance Program consistent with our commitment to high ethical standards of corporate conduct and compliance with regulatory and statutory requirements.

Definitions:

Compliance Program is fully described in the Compliance Program Description and approved by the Providence Board of Directors.

Workforce Member is defined as all caregivers, employees of affiliated organizations, board of directors, community board members, foundation board members, volunteers, students, independent contractors and other persons under direct control of a Providence entity, whether paid by Providence.

Policy:

Under the leadership of the Vice President/Chief Compliance Officer, the Compliance Program provides a supportive structure and applies to all workforce members. This program demonstrates the commitment of the Board and executive leadership to an effective compliance program and is based on the ethics and compliance program elements found in the United States Sentencing Commission's Federal Sentencing Guidelines, in conjunction with the compliance program guidance for various types of health care entities as issued by the Department of Health & Human Services, Office of Inspector General.

The Providence Board of Directors reaffirms their commitment to the Compliance Program annually.

Requirements:

Consistent with the Mission, Vision and Values of our organization, the Compliance Program establishes a framework to assist our workforce members in understanding the expectations related to integrity and being compliant with rules, regulations, organization policies and standards, and requirements that apply when providing services for our patients and consumers. The Compliance Program includes, at a minimum, the following components:

1. *Written policies and procedures* that describe compliance expectations, including a Code of Conduct distributed across the family of organizations which includes all caregivers. Our Code of Conduct requires all workforce members to report any known or suspected violations of law or regulation.
    - A Code of Conduct distributed across the family of organizations which includes all caregivers. Our Code of Conduct requires all workforce members to report any known or suspected violations of law or regulation
    - To ensure compliance with contractual and regulatory requirements, Compliance will conduct an annual review of all Compliance owned policies.
    - A Compliance Program Description;
        - Policies that include key risk areas that the Compliance Program administers or has ownership of related to the process occurring, i.e.: Conflicts of Interest
        - Compliance infrastructure including committees and oversight; Auditing and Monitoring program; and
        - An educational framework to deliver consistent mandatory compliance education across the organization which includes:
            - Delivery of general compliance and fraud, waste and abuse (FWA) training for new hires within 90 days and

also delivery and tracking of annual and routine compliance education.

  - Determination of education topics such as general compliance, privacy, and information security topics and/or job-specific education for caregivers, compliance high risk areas such as fraud, waste and abuse, etc.

- Communication, reporting
  - Compliance Program orientation for new caregivers;
  - Social media, email, other media to communication compliance topics, information

- Management of the anonymous mechanism for reporting and expectations of compliance when concerns are identified;
  - Communication lines accessible to workforce members that allow integrity and compliance concerns to be reported anonymously, the organization has an Integrity Hotline and Integrity Online, our web-based reporting tool.
  - Defining the process for investigating integrity and compliance concerns
  - Defining the process for reporting to appropriate agencies
  - Additional options for reporting concerns and having questions answered including contacting the following sources directly:
    -Department Managers and Supervisors;
    -Human Resources/Legal;
    -Local/Regional compliance/privacy staff;
    -Chief Compliance Officer;
    -Chief Operations Officer.
  - Response and Prevention Process related to compliance concerns raised
    -Assuring there is a policy of non-retaliation for good faith participation by any caregiver that reports concerns and/or assists in an investigation about actual or potential wrong-doing, including violations of law, regulation, policy, or our Code(s) of Conduct.
    -Assuring there is a policy related to obstructing an investigation.

2. Chief Compliance Officer appointment and Oversight Committee and committee infrastructure to assure Compliance Program is effectively implemented and managed.
3. All caregivers have a duty to report any suspected wrongdoing or violation of applicable laws, regulations or policies. Workforce members who fail to fulfill this duty may be subject to corrective action pursuant to policy. Appropriate disciplinary policies that are consistently applied and provide for appropriate discipline or sanctions that are

enforced.

4. A risk assessment process to identify, prioritize and manage key compliance risks resulting in an annual work plan. The process, at a minimum, includes:
    - Interviews with organization leaders;
    - Review of applicable guidance/information from enforcement, cognizant agencies, etc.; and
    - Trends provided by compliance risk data generated from self-monitoring, and internal and external audit activities.

References:

Compliance Program Description
Providence Code of Conduct
PSJH-CPP-711 Fraud, Waste, Abuse Prevention and Detection
PSJH-CPP-722 Code of Conduct Policy
PSJH-CPP-733 Non-Retaliation Policy
PSJH-CPP-735 Investigations Policy
PSJH-CPP-736 Compliance Hotline Policy
PSJH-CPP-741 Disclosure Program Policy
PSJH-CPP-743 Compliance Reporting Obligations Policy
PSJH-CPP-850 General Privacy Policy
PSJH-CPP-851 Privacy Sanctions Policy
Federal Sentencing Guidelines - Ethics and Compliance Program Elements
Office of Inspector General (OIG) General Compliance Program Guidance (GCPG)

Attachments:

No Attachments.

Applicability:

[1] For purposes of this policy, “Affiliates” is defined as any entity that is wholly owned or controlled by Providence St. Joseph Health (PSJH), Providence Health & Services, St. Joseph Health System, Western HealthConnect, Covenant Health Network, Grace Health System, Providence Global Center*, NorCal Health Connect, or is jointly owned or controlled by PSJH or its Affiliates and bears the Providence, Swedish Health Services, St. Joseph Health, Covenant Health, Grace Health System, Kadlec, or Pacific Medical Centers names (includes Medical Groups, Home and Community Care, etc.). *Policies and/or procedures may vary for our international affiliates due to regulatory differences.

Approval Signatures

Step Description	Approver	Date
Policy Owner	David Lane: Chief Compliance Officer [CJ]	11/2024
Policy Contact	Karen Coleman: Director Compliance	11/2024

Applicability

AK - Credena Health, AK - Providence Alaska MC, AK - Providence Kodiak Island MC, AK - Providence Medical Group, AK - Providence Seward MC, AK - Providence St. Elias Specialty Hospital, AK - Providence Valdez MC, CA - Credena Health, CA - Healdsburg Hospital, CA - Petaluma Valley Hospital, CA - Physician Enterprise Northern, CA - Physician Enterprise Southern, CA - Providence Cedars-Sinai Tarzana MC, CA - Providence Holy Cross MC, CA - Providence LCM MC San Pedro, CA - Providence LCM MC Torrance, CA - Providence Mission Hospitals, CA - Providence Queen of the Valley Medical Center, CA - Providence Redwood Memorial Hospital, CA - Providence Saint John's Health Center, CA - Providence Saint Joseph MC, Burbank, CA - Providence Santa Rosa Memorial Hospital, CA - Providence St. Joseph Hospital - Eureka, CA - Providence St. Joseph Hospital Orange, CA - Providence St. Jude Medical Center, CA - Providence St. Mary Medical Ctr Apple Valley, MT - Credena Health, MT - Providence St. Joseph MC, Polson, MT - St. Patrick Hospital, NM - Covenant Hobbs Hospital, OR - Credena Health, OR - Providence Ctr for Medically Fragile Children, OR - Providence Health Oregon Labs, OR - Providence Hood River Memorial Hospital, OR - Providence Medford MC, OR - Providence Medical Group, OR - Providence Milwaukie Hospital, OR - Providence Newberg MC, OR - Providence Portland MC, OR - Providence Seaside Hospital, OR - Providence St. Vincent MC, OR - Providence Willamette Falls MC, PHCC - Home & Community Care, PHCC - Home Health, PHCC - Home Medical Equipment, PHCC - Hospice, PHCC - Infusion/Pharmacy, PHCC - PACE, PHCC - Palliative Care, PHCC - Skilled Nursing/Assisted Living, Providence, Providence Express Care, Providence Global Center, Providence Physician Enterprise, Providence Traditional Health Workers, TX - Covenant Children's Hospital, TX - Covenant Health - ACO, TX - Covenant Health Partners, TX - Covenant Hospital Levelland, TX - Covenant Hospital Plainview, TX - Covenant Medical Center, TX - Covenant Medical Group, TX - Covenant Specialty Hospital, TX - Grace Clinic, TX - Grace Surgical Hospital, WA - Credena Health, WA - EWA Providence Medical Group, WA - Kadlec Regional Medical Center, WA - NWR Providence Medical Group, WA - PacMed, WA - Providence Centralia Hospital, WA - Providence DominiCare, WA - Providence Holy Family Hospital, WA - Providence Mt. Carmel Hospital, WA - Providence Regional MC Everett, WA - Providence Sacred Heart Med Ctr & Children's, WA - Providence St. Joseph's Hospital, WA - Providence St. Luke's Rehabilitation Medical, WA - Providence St. Mary MC, WA - Providence St. Peter Hospital, WA - SWR Providence Medical Group, WA - Swedish Medical Center, WA - Swedish Medical Group, WA - USFHP

Standards

No standards are associated with this document

Status **Active** PolicyStat ID **16990010**

Origination	01/2011	Owner	David Lane: Chief Compliance Officer
Last Approved	11/2024	Policy Area	Compliance
Effective	11/2024	Applicability	Providence Systemwide + PGC
Last Revised	11/2024		
Next Review	11/2025		

PSJH-CPP-722 Code of Conduct

Executive Sponsor:	Erik Wexler, President/CEO
Policy Owner:	David Lane, VP, Chief Compliance Officer
Contact Person:	Karen Coleman, Director, Compliance Services

Scope:

This policy applies to the not-for-profit, non-profit entities of Providence and its Affiliates[1] (collectively known as "Providence") and their workforce members (caregivers, professional staff, and members of the Providence System Board; Community Boards; and Foundation Boards, trustees, volunteers, trainees, interns, apprentices, students.), independent contractors, vendors and all other individuals working at the ministry, whether they are paid by or under the direct control of the facility; employees of affiliated organizations (collectively, "workforce members"). Where an organization is not wholly or majority owned, exceptions may apply.

☑ Yes ☐ No Is this policy applicable to Providence Global Center (PGC) caregivers?

This is a governance level policy, vetted by Executive Council with a recommendation for approval by the Providence Board, and signed by the appropriate delegate.

Purpose:

To define personal and professional standards of conduct and acceptable behaviors for all workforce members, while carrying out assigned responsibilities within Providence. This policy, along with the Code of Conduct, shall guide workforce members in business interactions with interested parties (e.g., suppliers, vendors, physicians, donors, politicians, etc.).

Definitions:

Compliance Program is fully described in the Compliance Program Description approved by the Board of Directors.
Workforce Member is defined as all caregivers, professional staff, and members of the Providence System Board; Community Boards; and Foundation Boards, trustees, volunteers, trainees, interns, apprentices, students.), independent contractors, vendors and all other individuals working at the ministry, whether they are paid by or under the direct control of the facility; employees of affiliated organizations (collectively, “workforce members”).

Policy:

Providence maintains a Code of Conduct (The Code) approved by the PSJH Board of Directors/ Board of Trustees for its workforce members across the Providence family of organizations. This document describes and encourages behaviors in support of our mission, vision, and values to prevent and halt unethical or unlawful behavior as soon as reasonably possible after discovery. The Code provides Providence workforce members an understanding of expectations and their responsibilities as a Providence employees including their responsibility to report concerns.

Requirements:

1. The Code will be provided either in paper format or electronically to caregivers prior to hire but in no event later than 90 days of hire. Thereafter, a link will be provided to the Code whenever an update occurs, and will also be included within the annual mandatory compliance education.
2. It is the responsibility of workforce members to:
    a. Act in a manner consistent with the Code, its supporting policies and procedures as well as applicable federal, state and local laws, and regulations;
    b. Support the Code by holding others accountable to the standards of conduct established in the Code;
    c. Seek clarification of any part of the Code that is not understood or where a question arises; and
    d. Report concerns or alleged violations promptly as outlined in the Code
3. The Code is available to workforce members in printed and/or electronic form in languages determined by management to meet the needs of Providence's diverse workforce.
4. The Code is reviewed and updated periodically.
5. Generally, the Code will cover the following topics:
    a. Mission and values.
    b. Purpose of the Code.

c. Information on the Compliance Program.

d. How to report a concern.

e. Non-retaliation and corrective action.

f. Commitment to ethical and legal business practices.

6. Other ministry specifics operationalizing the Providence Code of Conduct may be implemented as long as they do not conflict with the Providence Code of Conduct.

References:

Providence Code of Conduct

Attachments:

No attachments.

Applicability:

[1]For purposes of this policy, “Affiliates” is defined as any not-for-profit or non-profit entity that is wholly owned or controlled by Providence St. Joseph Health (PSJH), Providence Health & Services, St. Joseph Health System, Western HealthConnect, Kadlec, Covenant Health Network, Grace Health System, Providence Global Center*, NorCal HealthConnect, or is a not-for-profit or non-profit entity majority owned or controlled by PSJH or its Affiliates and bears the Providence, Swedish Health Services, St. Joseph Health, Covenant Health, Grace Health System, Kadlec, or Pacific Medical Centers names (includes Medical Groups, Home and Community Care, etc.). *Policies and/or procedures may vary for our international affiliates due to regulatory differences.

Attachments

📎 COC FINAL 2023.pdf

Approval Signatures

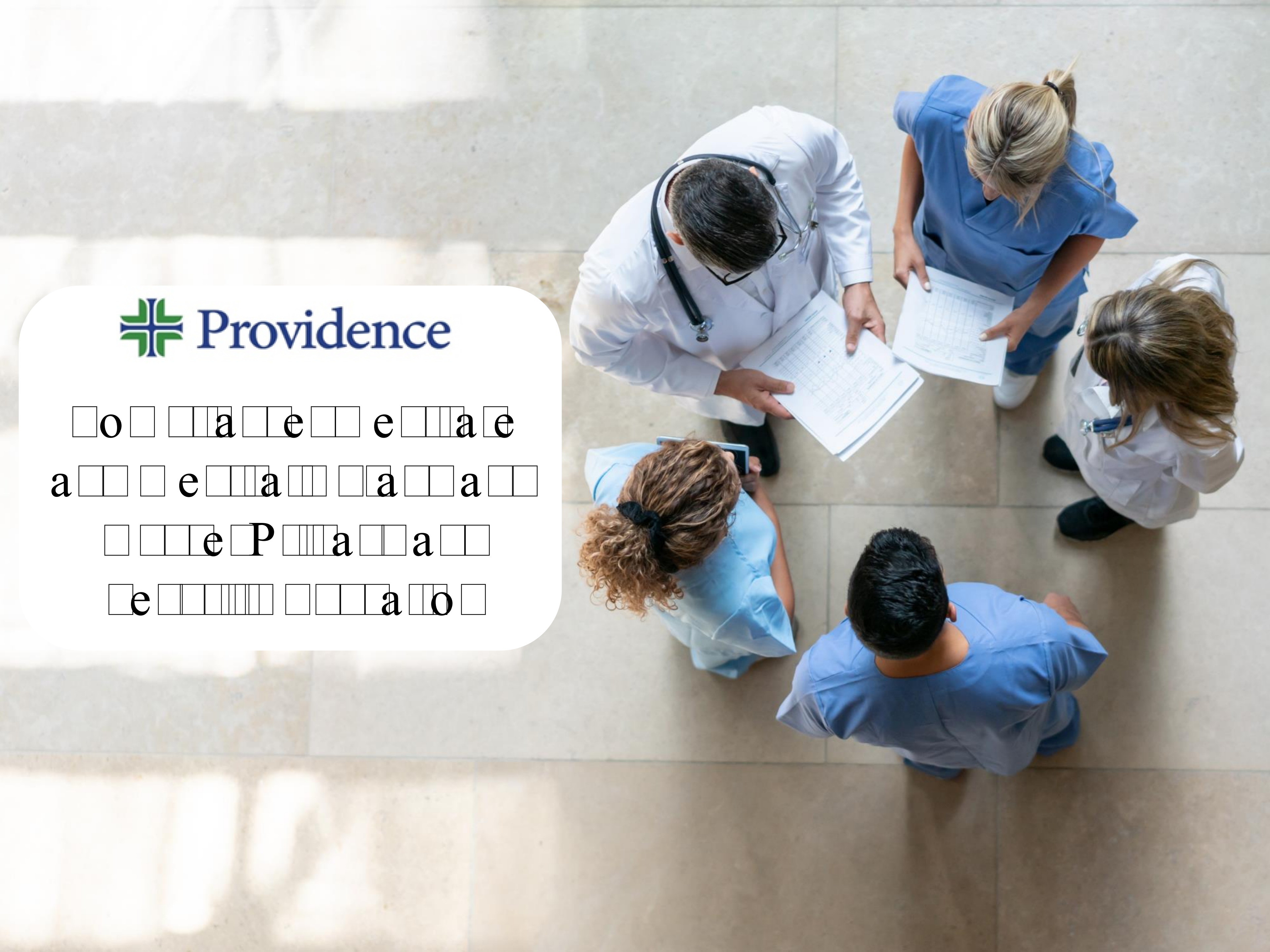
Step Description	Approver	Date
Policy Owner	David Lane: Chief Compliance Officer [CJ]	11/2024
Policy Contact	Karen Coleman: Director Compliance	11/2024

Applicability

AK - Credena Health, AK - Providence Alaska MC, AK - Providence Kodiak Island MC, AK - Providence Medical Group, AK - Providence Seward MC, AK - Providence St. Elias Specialty Hospital, AK - Providence Valdez MC, CA - Credena Health, CA - Healdsburg Hospital, CA - Petaluma Valley Hospital, CA - Physician Enterprise Northern, CA - Physician Enterprise Southern, CA - Providence Cedars-Sinai Tarzana MC, CA - Providence Holy Cross MC, CA - Providence LCM MC San Pedro, CA - Providence LCM MC Torrance, CA - Providence Mission Hospitals, CA - Providence Queen of the Valley Medical Center, CA - Providence Redwood Memorial Hospital, CA - Providence Saint John's Health Center, CA - Providence Saint Joseph MC, Burbank, CA - Providence Santa Rosa Memorial Hospital, CA - Providence St. Joseph Hospital - Eureka, CA - Providence St. Joseph Hospital Orange, CA - Providence St. Jude Medical Center, CA - Providence St. Mary Medical Ctr Apple Valley, MT - Credena Health, MT - Providence St. Joseph MC, Polson, MT - St. Patrick Hospital, NM - Covenant Hobbs Hospital, OR - Credena Health, OR - Providence Ctr for Medically Fragile Children, OR - Providence Health Oregon Labs, OR - Providence Hood River Memorial Hospital, OR - Providence Medford MC, OR - Providence Medical Group, OR - Providence Milwaukie Hospital, OR - Providence Newberg MC, OR - Providence Portland MC, OR - Providence Seaside Hospital, OR - Providence St. Vincent MC, OR - Providence Willamette Falls MC, PHCC - Home & Community Care, PHCC - Home Health, PHCC - Home Medical Equipment, PHCC - Hospice, PHCC - Infusion/Pharmacy, PHCC - PACE, PHCC - Palliative Care, PHCC - Skilled Nursing/Assisted Living, Providence, Providence Express Care, Providence Global Center, Providence Physician Enterprise, Providence Traditional Health Workers, TX - Covenant Children's Hospital, TX - Covenant Health - ACO, TX - Covenant Health Partners, TX - Covenant Hospital Levelland, TX - Covenant Hospital Plainview, TX - Covenant Medical Center, TX - Covenant Medical Group, TX - Covenant Specialty Hospital, TX - Grace Clinic, TX - Grace Surgical Hospital, WA - Credena Health, WA - EWA Providence Medical Group, WA - Kadlec Regional Medical Center, WA - NWR Providence Medical Group, WA - PacMed, WA - Providence Centralia Hospital, WA - Providence DominiCare, WA - Providence Holy Family Hospital, WA - Providence Mt. Carmel Hospital, WA - Providence Regional MC Everett, WA - Providence Sacred Heart Med Ctr & Children's, WA - Providence St. Joseph's Hospital, WA - Providence St. Luke's Rehabilitation Medical, WA - Providence St. Mary MC, WA - Providence St. Peter Hospital, WA - SWR Providence Medical Group, WA - Swedish Medical Center, WA - Swedish Medical Group, WA - USFHP

Standards

No standards are associated with this document



Providence

□o□ □□□a□□e□□ e□□□a□e
a□□ □ e□□□a□□□ □□a□□a□□
□ □□□e□P□□□□a□□a□□
□e□□□□□□□ □□□□a□o□

Faculty Disclosure Summary

The content of this activity is not related to products or services of an ACCME-defined ineligible company; therefore no one in control of content has a relevant financial relationship to disclose and there is no potential for conflicts of interest. All planners and presenters attested that their content suggestions and/or presentation(s) will provide a balanced view of therapeutic options and will be entirely free of promotional bias. All presentations have been reviewed by a planner with no conflicts of interest to ensure that the content is evidence-based and unbiased.

□he information provided addresses several re□uirements of the Accreditation Council for Continuing □edical Education □ACC□E□to help ensure independence in C□E activities□Everyone in a position to control the content of a C□E activity must disclose all relevant financial relationships with ineligible companies to the C□E provider□□his information must be disclosed to participants prior to the beginning of the activity□Also, C□E providers must mitigate relevant conflicts of interest prior to the educational activity. The ACCME defines “ineligible companies” as those whose primary business is producing, marketing, selling, re□selling or distributing healthcare products used by or on patients□Among the exemptions to this definition are government organi□ations, non□health care related companies and non□profit organi□ations that do not advocate for commercial interests. Circumstances create a “conflict of interest” when an individual has an opportunity to affect CME content about products or services of an ineligible company with which he/she has a financial relationship□ACC□E focuses on financial relationships with ineligible companies in the 2□□month period preceding the time that the individual is being as□ed to assume a role controlling content of the C□E activity□ACC□E has not set a minimal dollar amount for relationships to be significant□ Inherent in any amount is the incentive to maintain or increase the value of the relationship. The ACCME defines “relevant financial relationships” as financial relationships in any amount occurring within the past 24 months that create a conflict of interest□

Accreditation with Commendation

CME Accreditation Information

□his activity has been planned and implemented in accordance with the accreditation re□uirements and policies of the Accreditation Council for Continuing □edical Education □ACC□E□through the □oint providership of Swedish □edical Center and Providence St□□oseph □ealth□Swedish □edical Center is accredited by the ACC□E to provide continuing medical education for physicians□

AMA PRA Category 1 Credits™

Swedish □edical Center designates this internet enduring material for a maximum of 0□□5 *AMA PRA Category 1 Credits™*□ Physicians should claim only the credit commensurate with the extent of their participation in the activity□

Compliance At Providence

- [illegible]

- The Compliance program's main function is to recognize and prevent regulatory risk. [illegible]

- [illegible]

- [illegible]

- Compliance Services manages Providence's Code of Conduct, compliance policies, [illegible]

Chief Compliance Officer (CCO)

- ✓ Providence has designated a CCO who is responsible for oversight of the Compliance Program.
- ✓ The CCO strives to implement effective compliance training, auditing, reporting, screening, and investigation programs.
- ✓ The CCO is available to workforce members to answer compliance questions.

Chief Compliance Officer,
David Lane, Ph.D.

Providence

Code of Conduct [illegible]

[illegible]

The Compliance Program owns and is responsible for the upkeep of our organization's **Code of Conduct**. All workforce members are asked to review and agree to abide by the COC on a yearly basis while working for Providence.

The COC was designed in a way to make it accessible for all workforce members. The COC provides overviews on important topics such as:

- Culture of diversity and respect
- Quality of care and patient safety
- Ethical and legal standards
- Safeguarding patient information and protecting privacy and confidentiality
- Compliance with applicable federal and state laws and regulations and policies
- Duty to report suspected violations and protection from retaliation

The COC reinforces our organizations values, which drive our actions and the principles that underline decision making. Therefore, the Code becomes the most important part of the organization's ethical framework.

Providence

Providence

September 2023

Doing the Right Thing Right

Culture of Diversity and Respect

We adhere to all laws and regulations and are committed to a workplace culture where all individuals are treated with respect and dignity, regardless of protected characteristics, as defined by local, state, or federal law, including but not limited to race, color, religious creed (including religious dress and grooming practices), national origin (including certain language use restrictions), ancestry, disability (mental and physical including HIV and AIDS), medical condition (including cancer and genetic characteristics), genetic information, marital status, age, sex (which includes pregnancy, childbirth, breastfeeding and related medical conditions), gender, gender identity, gender expression, sexual orientation, and military and veteran status. POLICY

Quality of Care and Patient Safety

We commit to provide the best, *compassionate* care and service every time and strive to meet and exceed national standards for quality and patient *safety*. Workforce members have the responsibility and obligation to report any Quality of Care and Patient Safety issues. POLICY

Stewardship of Resources

We commit to effective stewardship of resources in support of patient care and organizational goals and only use resources for legitimate business purposes. POLICY

Conflicts of Interest (COI) Commitment

We will avoid actual or perceived COI and agree to disclose any outside interests or activities, contracts, and relationships that may be in conflict to the organization. We maintain impartial relationships with vendors, research sponsors, and contracts by not requesting or accepting gifts, cash, or cash equivalents. POLICY

Ethical and Legal Standards

We conduct ourselves in a professional and ethical manner in support of *justice* and will perform our job duties in accordance with all federal, state, and local laws. POLICY

Our Code of Conduct

Ways to report a compliance, privacy, or other concern

- Discuss the matter or concern with your immediate supervisor
- Discuss the matter or concern with your department leader
- Discuss with your HR Partner, HR Service Center, or send report via HR Portal
- Contact your local or regional compliance or privacy representative
- Call the 24/7 Integrity Hotline at 888-294-8455 or use Integrity Online, our Web-based reporting option
- For Caregivers in India:
  - From an outside line, dial the direct access number: 000-117
  - At the English prompt dial 888-294-8455

You may report concerns anonymously

To report a quality or patient safety concern

- Discuss the matter or concern with your immediate supervisor
- Discuss the matter or concern with your department leader
- Discuss with your Quality leader or representative
- Call the 24/7 Integrity Hotline at 888-294-8455 or use Integrity Online, our Web-based reporting option
- HRP- High Reliability Platform
  - Must be on organization network to report

SPEAK UP FOR SAFETY

Safeguarding Patient Information and Protecting Privacy and Confidentiality

We take every precaution to safeguard patient information, and we will treat protected health information (PHI) of all with special care and follow all federal, state, and local laws. POLICY

Ethical Conduct of Research

We follow the highest ethical standards and comply with all laws, regulations, guidelines, and ethical directives (where applicable) that govern human, animal, and basic applied science research. POLICY

Licensure and Certification

We require all health care and education professionals to follow all federal, state, and local laws applicable to licensing, credentialing, and certification requirements. Individuals on the excluded provider lists cannot work for our organization. POLICY

Compliance with Applicable Federal and State Laws and Regulations, and Policies

We ensure *excellence* by requiring all parties that work for or on behalf of an employer within our family of organizations learn and follow all laws, regulations, and policies. POLICY

Fair Business Practices

We conduct ourselves ethically, honestly, and with *integrity* at all times. POLICY

Duty to Report Violations and Protection from Retaliation

It is every workforce member's responsibility to report, in good faith, any violation or suspected violations of our code, fraud, waste, abuse or quality or patient safety concerns as required. Providence's Non-Retaliation policy, and to an extent, government law, protects workforce members from retaliation or harassment for having raised concerns about actual or potential wrongdoing or misconduct ". POLICY

Our mission, vision, values, and promise provide guidance and inspiration as we deliver quality care, make sound, ethical choices, and meet our organizational goals. As workforce members, we are accountable for the integrity of our decisions and actions on the job. We are obligated to report any suspected violations or concerns. The Code of Conduct provides a foundation of expectations for us as we do our work each day.

A Roadmap for Physicians

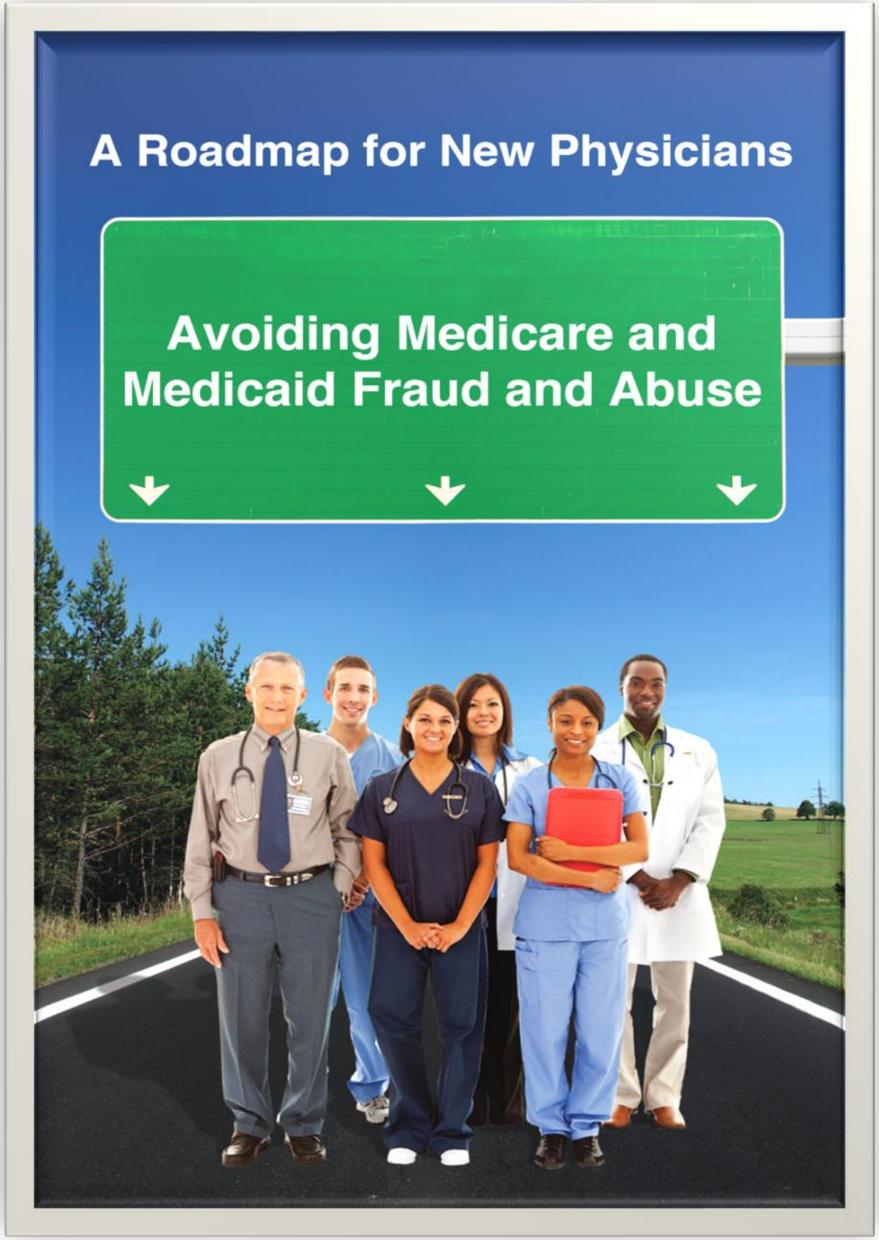
Avoiding Medicare and Medicaid Fraud and Abuse

To help you learn about these laws, the Office of Inspector General (OIG) has prepared a booklet entitled "A Roadmap for New Physicians: Avoiding Medicare and Medicaid Fraud and Abuse,".

OIG is the independent oversight agency for the United States Department of Health & Human Services. OIG's mission is to protect the integrity of the Federal health care programs and to promote the health and welfare of program beneficiaries.

This booklet provides an overview of the pertinent fraud and abuse laws and is a must read for your self-education.

Click the image to the right to download.


A Roadmap for New Physicians
Avoiding Medicare and Medicaid Fraud and Abuse

Office of Inspector General
U.S. Department of Health & Human Services

Health care fraud is a serious problem

- The Government spends almost a trillion dollars each year on the Medicare and Medicaid programs.
- Although there is no precise measure of health care fraud, experts estimate that fraudulent billings to the programs are in the range of 3–10 percent.
- **Healthcare fraud, waste, and abuse cost taxpayers' tens of billions of dollars per year, with Medicare and Medicaid fraud alone estimated to cost $300 billion annually.**
- Not only does fraud drain the taxpayers' money, but also it puts beneficiaries' health and welfare at risk by exposing them to unnecessary services and taking money away from needed patient care.
- When the Federal Government recovers money from fraud cases, it returns the money to the Medicare Trust Fund to pay for legitimate patient care.

Fraud includes obtaining a benefit through intentional misrepresentation or concealment of material facts.

Waste includes incurring unnecessary costs as a result of deficient management, practices, or controls.

Abuse includes any practice that is not consistent with the goals of providing patients with services that (1) are medically necessary, (2) meet professionally recognized standards, and (3) are fairly priced.

Fraud and Abuse Laws

[illegible]

1□ □he □ealth Care □raud Statute□

2□ □he □alse Claims Act□

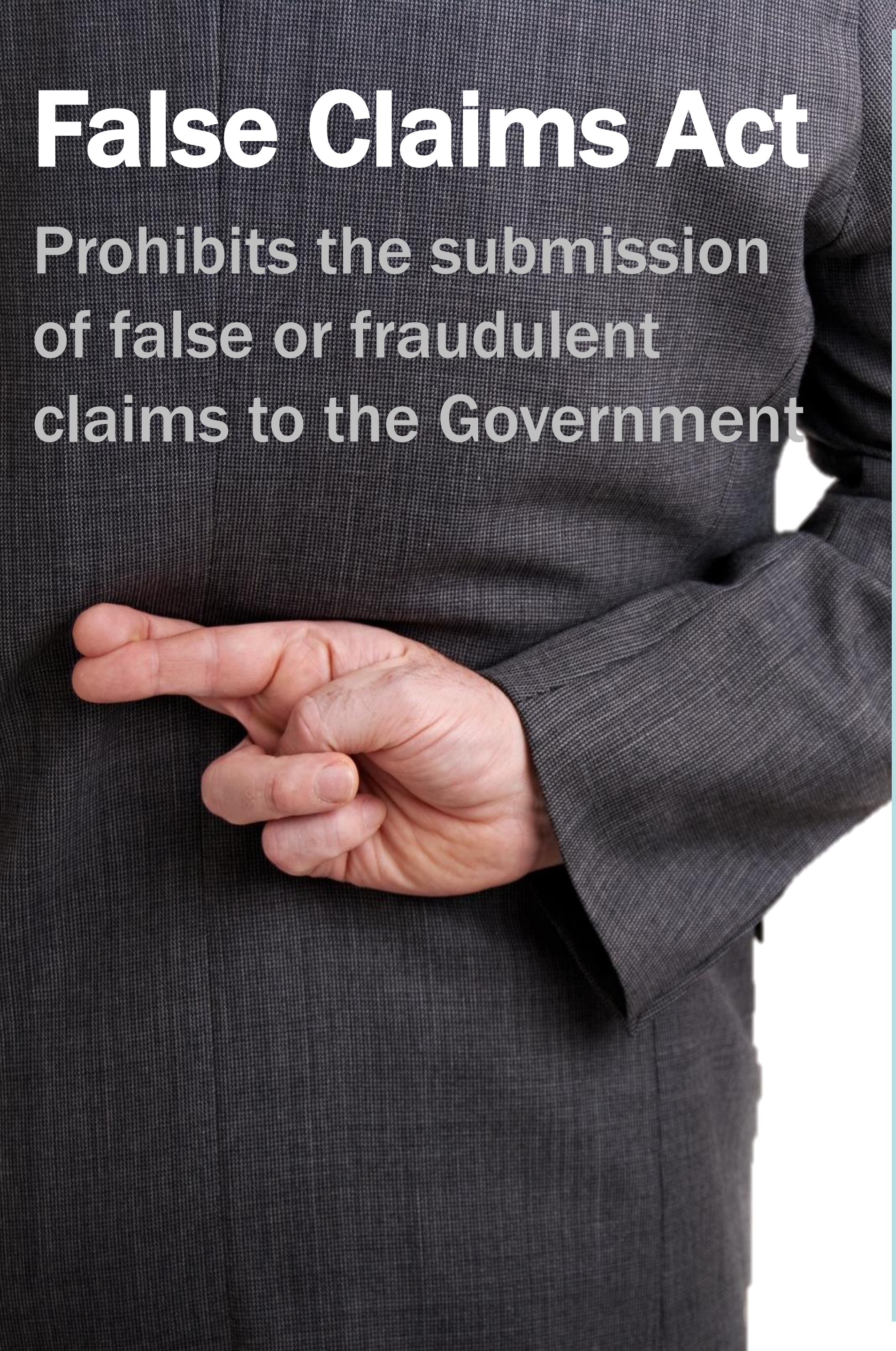
3□ □he Anti□□ic□bac□Statute□

□□ □he Patient Access and □edicare Protection Act□

5□ Exclusion Provisions□and

6□ □he Civil □onetary Penalties Law

[illegible]



False Claims Act

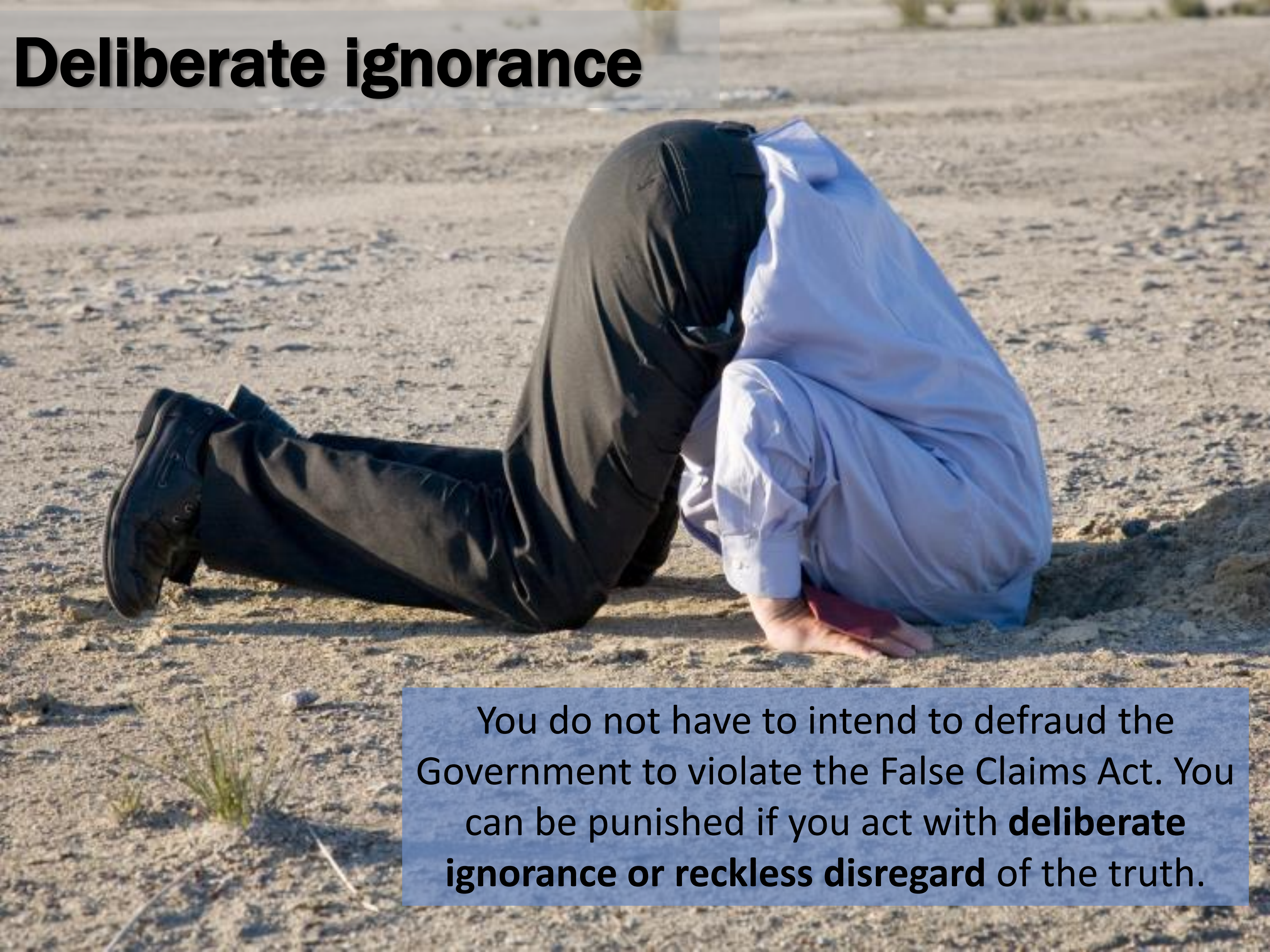
Prohibits the submission of false or fraudulent claims to the Government

Claims may be false if the service is not actually rendered to the patient, is provided but already covered under another claim, is miscoded, or is not supported by the medical record.

- For example, a hospital compensated its physicians in a way that violated the Stark Law against physician self-referrals therefore violating the False Claims Act. The hospital had submitted 21,730 false claims to Medicare with a total value of $39,313,065. The district court assessed 21,730 civil False Claims Act penalties. Ultimately, the hospital was on the hook for **$119,515,000** in False Claims.

For False Claims Act violations, you can be fined up to three times the program's loss, plus **$13,946 per claim**. And fines add up quickly because each claim can be a separate ground for liability.

Deliberate ignorance



You do not have to intend to defraud the Government to violate the False Claims Act. You can be punished if you act with **deliberate ignorance or reckless disregard** of the truth.

Incentives to Report Fraud

The False Claims Act also provides a strong financial incentive to whistleblowers to report fraud.

Whistleblowers can *receive up to 30 percent* of any False Claims Act recovery.

Often whistleblowers turn out to be ex-business partners, hospital or office staff, competitors, or even patients.

Anti-Kickback Statute (AKS)

The AKS is a federal criminal law. It prohibits offering or accepting kickbacks to generate health care business. As a result, violation of the AKS is a felony, punishable by ten years in jail and fines of $100,000 per violation.

The AKS applies to both payers and recipients of kickbacks. Whoever knowingly and willfully solicits or receives any remuneration directly or indirectly, overtly or covertly, in cash or in kind.

Anti-Kickback Statute

“Remuneration” is anything of value (including any discount, kickback, bribe, or rebate).

The law prohibits obvious kickbacks, like *cash for referrals*, as well as more subtle kickbacks, like *free rent, below fair market value rent, free clerical staff, or excessive compensation for medical directorships.*

Numerous physicians have been sanctioned for selling their product loyalty to drug or device companies or other vendors.

•An orthopedic surgeon was sentenced to 33 months in federal prison for accepting more than $315,000 in bribes and kickbacks for performing spinal surgeries at a now-defunct Long Beach hospital whose owner was imprisoned for committing workers’ compensation insurance fraud. The surgeon was also fined $20,000 and ordered to forfeit $316,597.

Anti-Kickback Statute (AKS) [42 U.S.C. § 1320a-7b(b)]

The AKS is a criminal law that prohibits the knowing and willful payment of "remuneration" to induce or reward patient referrals or the generation of business involving any item or service payable by the Federal health care programs (e.g., drugs, supplies, or health care services for Medicare or Medicaid patients).

- Remuneration includes anything of value and can take many forms besides cash, such as free rent, expensive hotel stays and meals, and excessive compensation for medical directorships or consultancies. In the Federal health care programs, **paying for referrals is a crime**.
- **Whoever knowingly and willfully solicits or receives any remuneration** (including any kickback, bribe, or rebate) directly or indirectly, overtly or covertly, in cash or in kind; additionally, **whoever knowingly and willfully offers or pays any remuneration** (including any kickback, bribe, or rebate) directly or indirectly, overtly or covertly, in cash or in kind to any person to induce such person **shall be guilty of a felony and upon conviction**.

As physicians, you owe your patients the benefit of your best clinical judgement.

Penalties for Kickbacks

Fines

Prison Time

- Violation of the Federal Anti-Kickback Statute (AKS) constitutes **a felony punishable by a maximum fine of $100,000, imprisonment up to 10 years, or both**. Conviction also will lead to mandatory exclusion from Federal health care programs, including Medicare and Medicaid. Liability under the Federal anti-kickback statute is determined separately for each party involved.
- Violation of the **AKS also triggers liability under the Civil Monetary Penalties Law (CMPL)**. The CMPL carries penalties of **up to $50,000 per kickback**, in addition to three times the amount of the remuneration. It also makes the resulting bills to the government false under the False Claims Act. As a result, the violator is responsible for three times the value of the bills, and a False Claims Act Penalty of **up to $27,894 per bill**.

Exclusion from Medicare and Medicaid

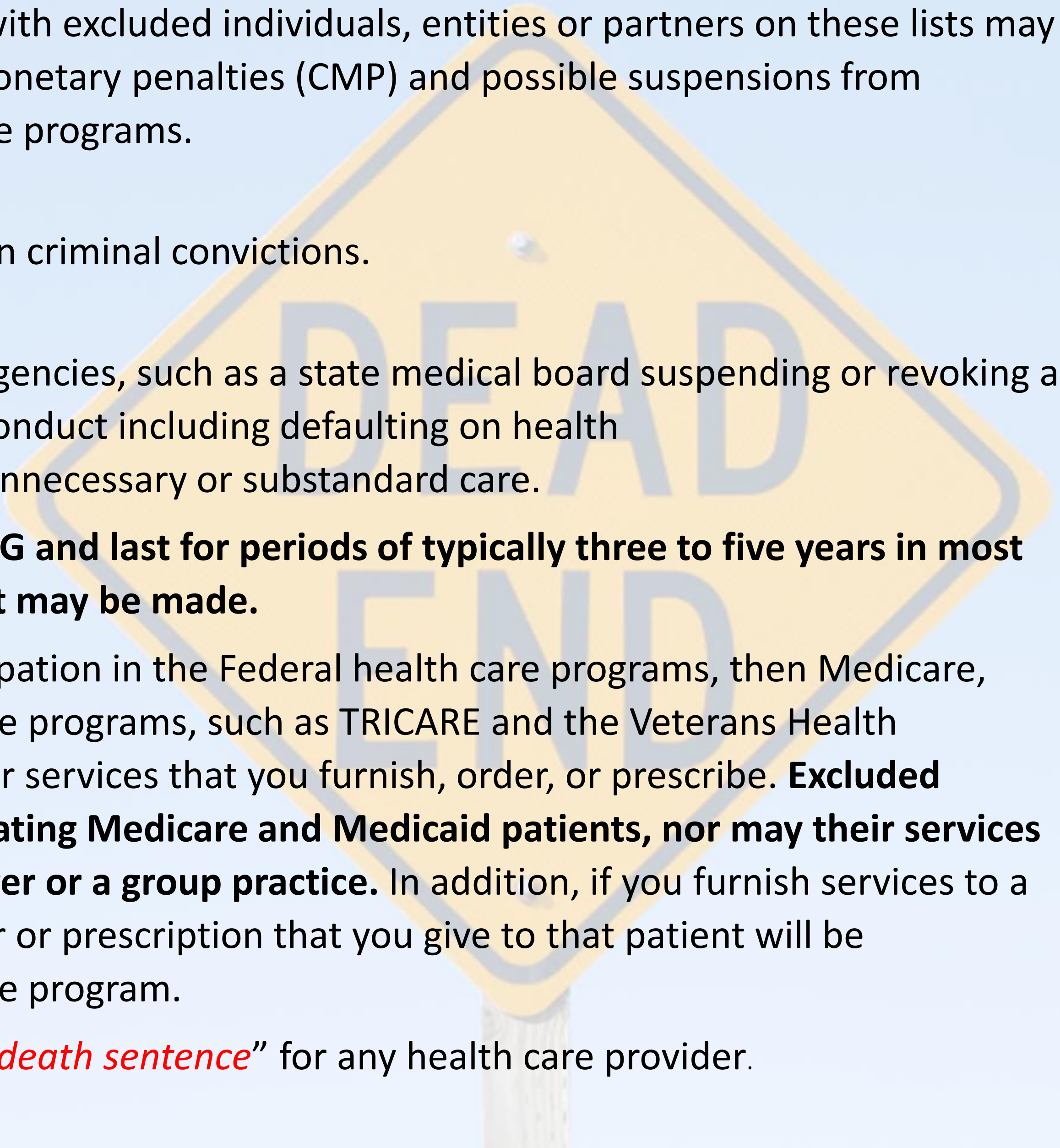
Healthcare agencies that do business with excluded individuals, entities or partners on these lists may be subject to penalties, fines or civil monetary penalties (CMP) and possible suspensions from participation in government health care programs.

- **Mandatory exclusions**
  - Imposed on the basis of certain criminal convictions.
- **Permissive exclusions**
  - based on sanctions by other agencies, such as a state medical board suspending or revoking a medical license, or other misconduct including defaulting on health education loans or providing unnecessary or substandard care.

Exclusions are handed down by the OIG and last for periods of typically three to five years in most cases before a potential reinstatement may be made.

If you are excluded by OIG from participation in the Federal health care programs, then Medicare, Medicaid, and other Federal health care programs, such as TRICARE and the Veterans Health Administration, will not pay for items or services that you furnish, order, or prescribe. **Excluded physicians may not bill directly for treating Medicare and Medicaid patients, nor may their services be billed indirectly through an employer or a group practice.** In addition, if you furnish services to a patient on a private-pay basis, no order or prescription that you give to that patient will be reimbursable by any Federal health care program.

Some refer to exclusion as a “*financial death sentence*” for any health care provider.



Exclusion Screening Requirements

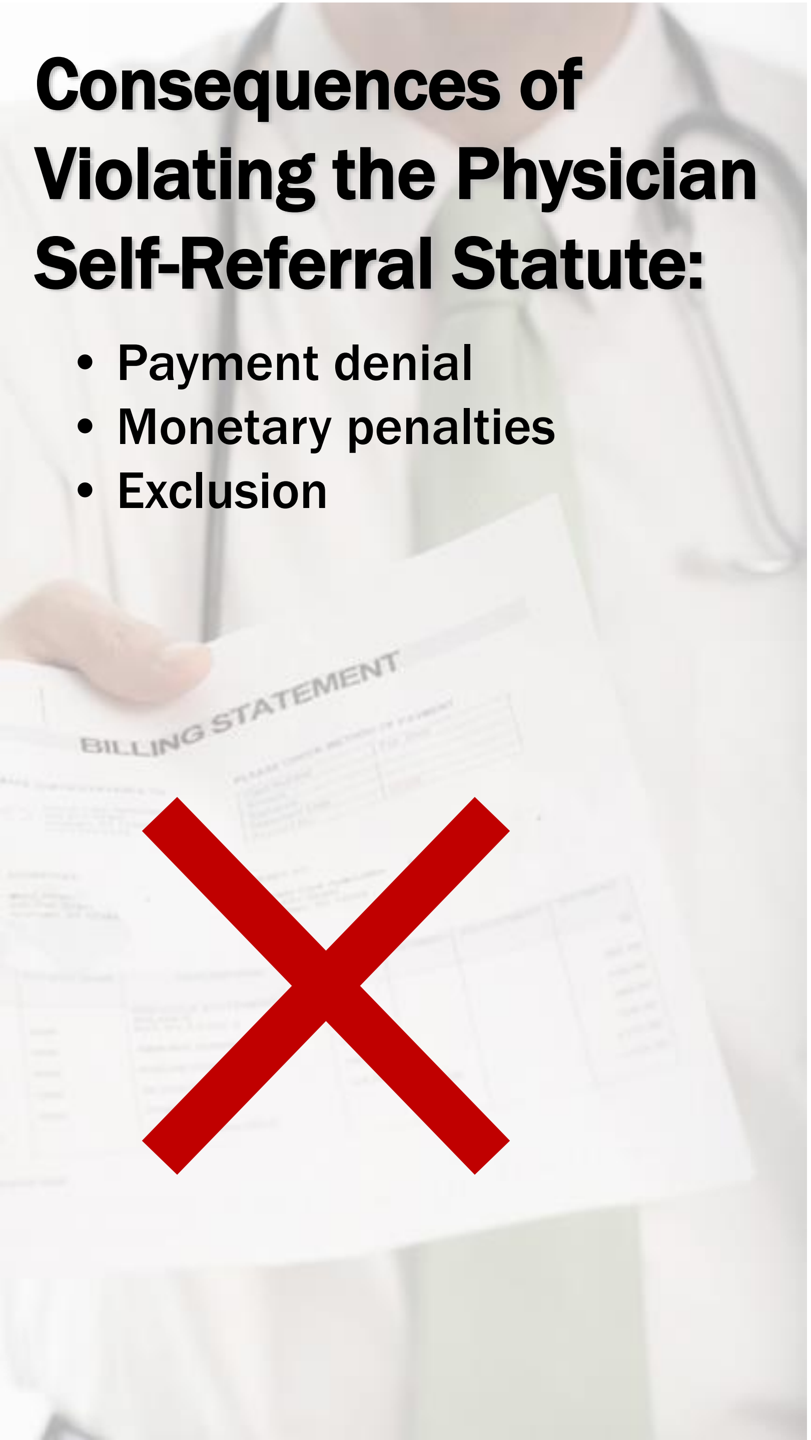
- In accordance with the Medical Staff Excluded Individual Checks policy Providence prohibits the credentialing and privileging of Medical Staff members who are deemed by a Federal and/or State agency as debarred, excluded or otherwise ineligible for participation in federal or state funded health care programs, or who have been convicted of a criminal offense related to health care.
- All Medical Staff members are screened against the Office of the Inspector General (OIG)'s List of Excluded Individuals and Entities (LEIE) and the General Services Administration (GSA)/System for Award Management (SAM), OFAC-SDN, CMS Preclusion, Medicare Opt Out, **and all State Medicaid exclusion lists** to ensure that none of these persons are excluded or become excluded from participation in federal programs.
- Screening occurs before hiring or contracting and then monthly thereafter. Those that are excluded can receive no payment from Federal health care programs for any items or services they furnish, order, or prescribe.
- Providence does not do business with any excluded individual or entity, as no payment can be received from a federal healthcare program such as Medicare or Medicaid for work done by an excluded individual.
- Over 33,000 health care providers have been barred from federal health care programs since 2010 due to fraud, license revocation, convictions for felony drug crimes, patient abuse and neglect or other issues.

Physician Self-Referral Law [42 U.S.C. § 1395nn]

- Commonly referred to as the *Stark Law*, prohibits physicians from referring patients to receive "designated health services" payable by Medicare or Medicaid from entities with which the physician or an immediate family member has a financial relationship, unless an exception applies. Financial relationships include both ownership/investment interests and compensation arrangements.
    - For example, if you invest in an imaging center, the Stark law requires the resulting financial relationship to fit within an exception or you may not refer patients to the facility and the entity may not bill for the referred imaging services.
- Financial relationships covered by this law include ownership/investment interests, as well as compensation relationships. This law applies to your financial relationships and those of your immediate family members.
- Designated health services include clinical laboratory services, physical therapy, and home health services, among others.

Consequences of Violating the Physician Self-Referral Statute:

- Payment denial
- Monetary penalties
- Exclusion



- The Physician Self-Referral Statute is a strict liability law, which means proof of **specific intent to violate the law is not required**.

- The entity submitting improper claims is subject to repayment of all amounts received from Medicare and Medicaid that are connected with the improper relationship and may be subject to additional penalties.

- Physicians who violate the law may be subject to monetary penalties as well as exclusion from participation in the Federal health care programs.

- If a referral is made violating the Stark law and payment is received by the entity providing the designated health service, penalties can include **civil penalties up to $15,000 for each unlawful referral**, exclusion from participation in federal health care programs, denial of payment for services, refunding of payments received, **a fine of up to $100,000** for each illegal cross-referral arrangement, and **civil penalties up to $10,000 per day for failing to report violations.**

Avoid violating the Anti-Kickback Statute and Physician Self-Referral Statute by fitting into a “safe harbor” or exception.

Many arrangements can be structured to avoid the risk of fraud. Additionally, the law provides for “safe harbors” and exceptions to the Anti-Kickback and Stark laws. To fit into an Anti-Kickback safe harbor or Stark law exception, you must fit squarely within the requirements. If the safe harbor or exception contains multiple elements or conditions, you must satisfy each element or condition.

For example, a full-time lease agreement between a physician and a provider to whom the physician refers patients can meet the *space rental safe harbor* if the agreement:

- is set out in writing and signed by the parties;
- covers all the premises rented by the parties;
- is for a term not less than 1 year;
- has an aggregate rental charge set in advance, is consistent with fair market value in arm’s length transactions, and does not take into account the volume or value of Federal health care program referrals; and,
- the aggregate space rented may not exceed the space that is reasonably necessary to accomplish the commercially reasonable business purpose of the rental.

Civil Monetary Penalties Law

You should also be aware that OIG may seek civil monetary penalties for a wide variety of abusive conduct, including presenting a claim that is false or fraudulent because it is for a medically unnecessary procedure. OIG also may impose civil monetary penalties for violating the Medicare assignment agreement by overcharging or double billing Medicare beneficiaries.

The adjusted civil penalty amounts for 2024 vary depending on the agency and the type of violation. Here are some examples:

1. **Department of Justice**: The adjusted civil penalties assessed or enforced by components of the Department range from **$7,256 to $84,852** for violations occurring after November 2, 2015.
2. **Federal Election Commission (FEC)**: Violations of federal campaign finance law can result in penalties ranging from **$7,028 to $82,188**.
3. **Department of Labor**: The 2024 civil money penalty amounts for labor-related violations are specified in a table published in the Federal Register.
4. **Executive Office of the President**: The inflation-adjusted penalty amount for 2024 is approximately **$13,946** when rounded to the nearest dollar.

Please note that these amounts apply to *specific violations and agencies*.

Reminder!

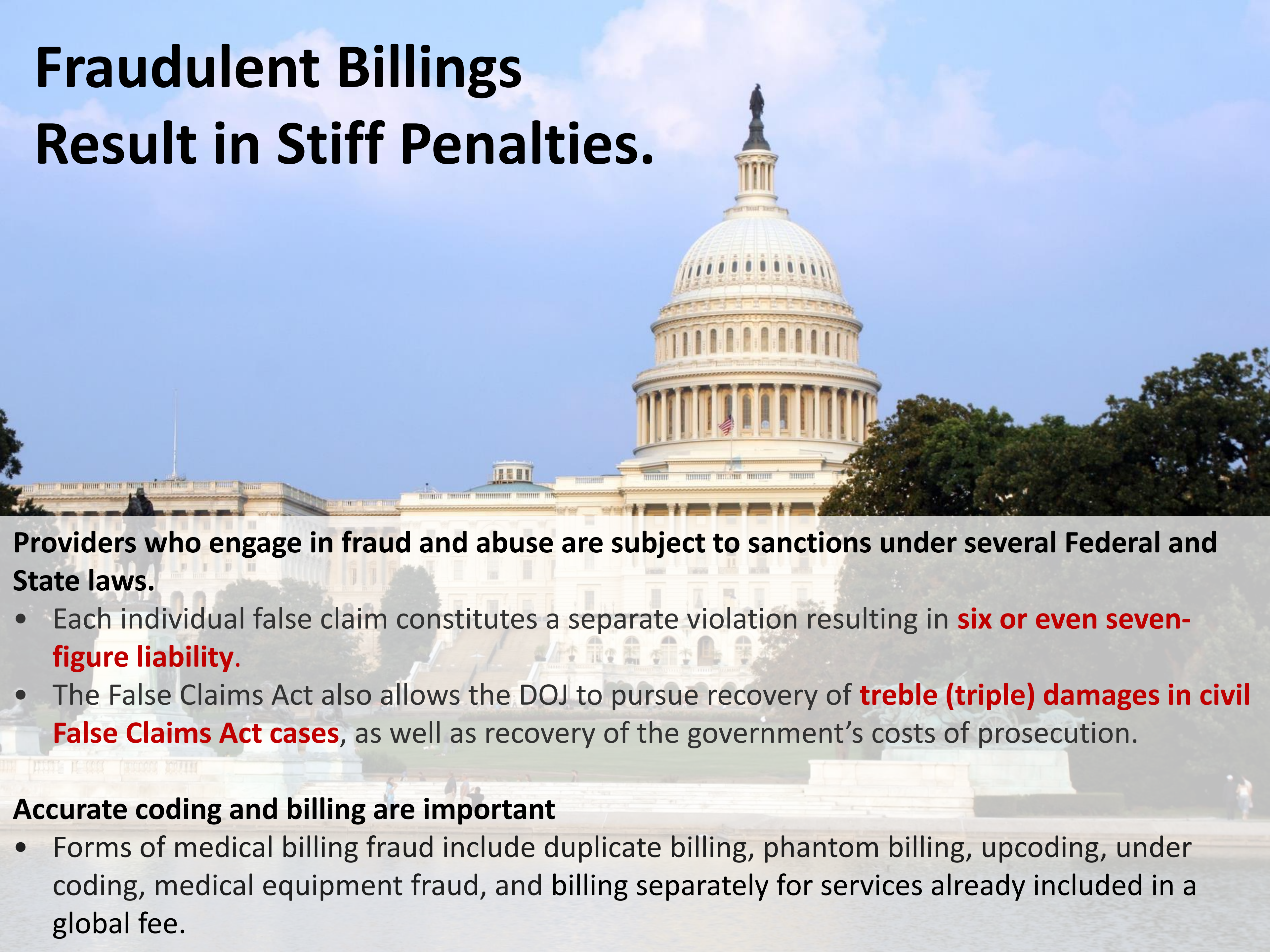
No matter your specialty or practice setting, as a physician you may develop relationships with three important groups. Your relationships with these groups will be subject to the provisions of the six key fraud and abuse laws.

1. **Payers**, like Medicare, Medicaid, patients, and private insurance companies;

2. **Other providers**, including physicians and hospitals; and

3. **Vendors**, including drug, biologic, and medical device companies.

Fraudulent Billings Result in Stiff Penalties.



Providers who engage in fraud and abuse are subject to sanctions under several Federal and State laws.

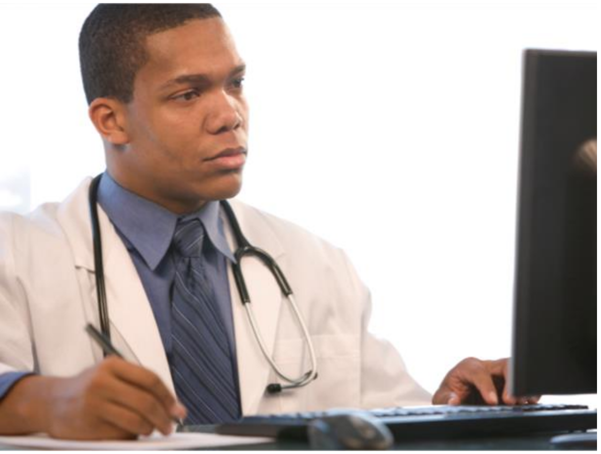
- Each individual false claim constitutes a separate violation resulting in **six or even seven-figure liability**.
- The False Claims Act also allows the DOJ to pursue recovery of **treble (triple) damages in civil False Claims Act cases**, as well as recovery of the government's costs of prosecution.

Accurate coding and billing are important

- Forms of medical billing fraud include duplicate billing, phantom billing, upcoding, under coding, medical equipment fraud, and billing separately for services already included in a global fee.

Accurate medical records are critical

The Medicare and Medicaid programs may review the patient’s medical records to verify the claim, as well as the quality of care. If the medical record does not support the claimed service, the claim may be denied.



Good documentation helps ensure quality patient care

Good documentation is also a quality of care issue. It helps ensure that your patients get the best possible clinical care from you and other providers who may rely on your records.

If you have questions about coding and documentation, ask someone you trust

Participating Physicians…

Most physicians bill Medicare as participating physicians and receive Medicare’s 80 percent directly from Medicare and bill patients for the remaining 20 percent.

This means that you accept the Medicare payment, plus any copayment or deductible Medicare requires the patient to pay, as the full payment. You may not require any extra payment from your patient.

In other words, you may not ask Medicare patients to pay a second time for services for which Medicare has already paid.

Non- Participating Physicians…

- Bill directly to patients
- Patients reimbursed by Medicare
- It is illegal to charge more than 15% above the Medicare rate

Future Business Relationships

Colleagues *Hospitals* *Nursing Homes*

Outside Investments

The Office of Inspector General ("OIG") has expressed concern that physician investments in medical device and distribution entities should be closely scrutinized under the fraud and abuse laws.

- Physicians are frequently approached with investment opportunities in enterprises related to the delivery of health care.
- Sometimes, you are a legitimate source of capital. Other times, you are a source of patient referrals.
- Because the return on an investment sometimes is used to offer kickbacks in exchange for referrals, you should be vigilant when considering health care business opportunities.
- You should send your patients to the provider that, in your medical judgment, can best meet their medical needs.
- Legal counsel may be helpful in understanding the purpose of the business venture and its associated risks.

Is the arrangement legitimate?

To avoid violation of the fraud and abuse laws, test the propriety of any proposed engagement by asking yourself the following questions:

- Does the company really need my particular expertise or input?
- Is the venture promising you high rates of return for little or no financial risk?
- Are you being asked to guarantee that you will refer patients or order services from the venture?
- Does the amount of money the company is offering seem fair and appropriate for what it is asking me to do?
- Is it possible the company is paying me for my loyalty so that I will prescribe its drugs or use its devices?

If you want to pursue an industry relationship but are not sure it is legitimate, take steps to learn whether the arrangement is proper.

As a physician, you may have opportunities to consult with or be a promotional speaker for the drug or medical device industry.

***Scrutinize* promotional speaking or consulting opportunities!**

Providence Policy Considerations

PSJH-CPP-718 **Vendor/Supplier Interactions**

Consulting Arrangements

Speaker's Bureau and Educational Events

PSJH-CPP-719 **Gifts, Gratuities, and Business Courtesies**

Honoraria/Honorarium and Consultations

Medical Directorships & Substantive Responsibility Requirements

Medical Director Agreement Considerations

- **Government Scrutiny**: Given the potential impact on referrals, government agencies closely examine medical director compensation arrangements.
- **Fair Market Value (FMV)**: When establishing medical directorships, it's essential to ensure that compensation is fair and reasonable.
- **Substantive and Well-Defined Roles**: Medical directorships should have clear responsibilities and expectations. These roles should be substantive, meaning they contribute significantly to the organization's functioning.
- **Uniform Contracts**: Consistency in contract terms is crucial. Organizations should use standardized agreements for medical directorships to maintain transparency and fairness.

Physicians can play an important role in ensuring quality of care by serving as medical directors. To be paid to serve as a medical director, you should spend an appropriate amount of time performing necessary services, including:

- actively overseeing clinical care in the facility;
- leading the medical staff to meet the standard of care;
- ensuring proper training, education, and oversight for physicians, nurses and other staff members; and
- identifying and addressing quality problems.

Free drug samples

If free drug samples are authorized in your clinic by local leadership; there are very specific criteria for use, and there should be a leadership committee at the local level determining if those practices are going to allow to have samples and what policies and procedures govern the sample drug process.

Free drug samples should be used for the purpose of testing for tolerance or titrating dose; they are not to be used as a means to providing financial assistance. Free drug samples should never be commingled with commercial stock drugs.

Gift reporting requirements

Although some physicians believe that free lunches, subsidized trips, and gifts do not affect their professional judgment, research shows that these types of perquisites and humans' natural desire to reciprocate can influence prescribing practices and generally affect how physicians act.

The Sunshine law requires public disclosure of gifts and limiting the types of gifts physicians may accept. This law ensure that certain activities are conducted openly and ethically, allowing public observation, participation, and access to records.

The Patient Protection and Affordable Care Act of 2010 requires drug, device, and biologic companies to publicly report nearly all gifts or payments they make to physicians since 2013. This information is posted on the Internet.

So, the public will know what gifts and payments a physician receives from industry. The "Internet test" is important to use in your relationships with the health care industry.

Giving Gifts to Providence Caregivers

Per Providence policy, directly employed caregivers of Providence are not permitted to accept gifts from independent physicians, even as a *Thank You* or around the holidays. Examples of gifts include:

- *Frequent* meals (breakfast, lunch, dinners)
- Tickets to events/shows
- Gift cards/Certificates/Vouchers
- Gifts that cannot be shared with the department
    - Electronics
    - Jewelry
    - Clothing items/accessories

Providence's Disclosure Program
Reporting Concerns

The purpose of the *Providence Disclosure Program* is to foster a culture of integrity, transparency, and accountability within our family of organizations. This program is designed to support the identification, correction, and prevention of compliance and quality issues, helping ensure the highest standards of ethical and legal conduct and patient care. It aims to empower all workforce members to speak up and report compliance and quality of care related issues and concerns confidentially and without fear of retaliation. *PSJH-CPP-741 Disclosure Program*

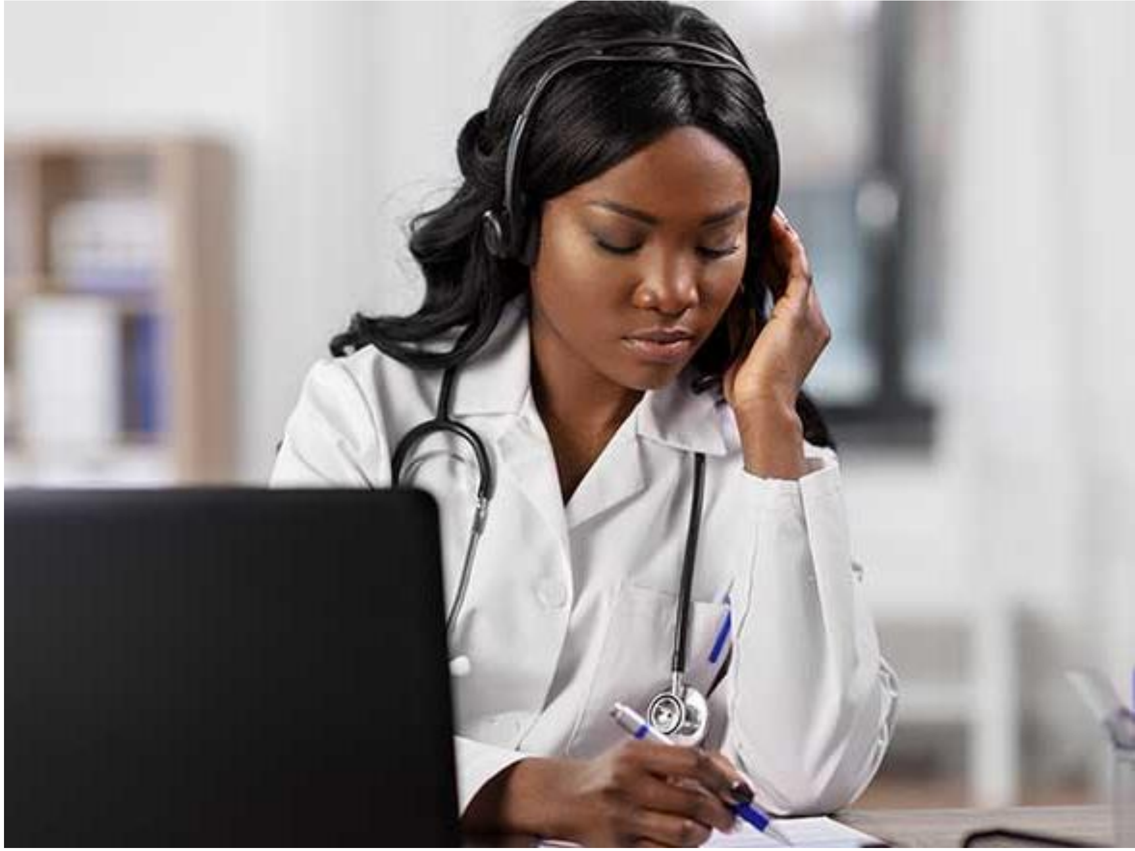
Integrity Hotline

1□888□294□8455

High Reliability Platform (HRP)

SPEAK UP
FOR SAFETY

More Ways to Report FWA Concerns



You can also report suspected cases of fraud, waste, or abuse [illegible] programs [illegible] the U.S. Department of Health and Human Services Office of Inspector General electronically through the Office of Inspector General's Complaint Portal, available at https://oig.hhs.gov/fraud/report-fraud/index.asp or by mail or phone at:

U.S. Department of Health and Human Services Office of Inspector General
ATTN: OIG HOTLINE OPERATIONS P.O. Box 23489 Washington, DC 20026

Phone: 1-800-HHS-TIPS (1-800-447-8477) or 1-800-377-4950 (TTY)

Privacy Compliance at Providence

- ➢ **Mission and Values:** Privacy is about respecting individuals - Safeguarding information is the “right thing to do” and our patients expect it
- ➢ **Legal and Regulatory:** The risk of civil monetary penalties and litigation is reduced when we comply with privacy requirements
- ➢ **Quality of Care:** Patient confidence in privacy promotes communication/ transparency for higher quality of care
- ➢ **Reputation and Viability:** Privacy creates an environment of trust for our patients

Know the 18 Patient Identifiers

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 (tattoos)
18. Any other unique identifying number, characteristic, or code (unique pictures with elements known to patient)

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—includes nurses, labs, technicians, etc.

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.

Examples of Sharing with Others

A physician 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 physician 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 physician may give information about a patient's mobility limitations to the patient's sister who is driving the patient home from the hospital.

Providence

Examples of Sharing When the Patient Cannot Authorize

A surgeon who did emergency surgery on a patient may tell the patient's spouse about the patient's condition while the patient is unconscious.

A pharmacist may give a prescription to a patient's friend who the patient has sent to pick up the prescription.

A health care provider may give information regarding a patient's drug dosage to the patient's health aide who calls the provider with questions about a prescription.

Providence

Access to EPIC and Other Information Systems

Access is granted based on job role

Access is monitored and recorded 24/7

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 up to and including termination

Impermissible Uses of EPIC

Using *any part* of the Electronic Health Record (EHR) to view a patient's record including their name and/or address only without a Providence business reason. The fact that an individual is/was a patient is protected health information. Follow query procedures to avoid accessing the wrong record.	*Includes birthdays, addresses, etc. even when asked by co-worker, family, etc.*
Searching, monitoring, accessing medical information for purposes of curiosity/concern.	*Includes co-worker, person of interest (people in the news, celebrities, etc.), family member, etc. This includes viewing census or ED status boards when doing so is not part of your job role.*
Using census boards/track boards, appointment desk, or other modules in the EHR outside your job role.	*Monitoring for admissions to your unit when this is not your role; making appointments for family, self or friends, locating them in hospital, checking ED wait times, etc.*

Impermissible Uses of EPIC (cont.)

Using patient chart for training purposes.	*Includes co-worker charts, even with their permission.*
Circumventing ROI/HIM processes to obtain copies of medical records for self or others.	*Including records needed for litigation, research, etc.*
Sharing credentials or not logging off before workstation is used by another user.	*Utilize the IT Service Desk. You are responsible for all access made under your user credentials – protect them!*

Privacy and Patient Rights Safeguards: *What Should You Do?*

Verify patient identity by using 3 identifiers. Many patients share full names and dates of birth and errors cause significant billing issues for patients along with privacy concerns.

Be cautious with verbal conversations whether in treatment areas or in public areas. Know the audience listening.

Escalate *all requests* by patients promptly to avoid missing legal deadlines (i.e.; requests for medical record access or changes to medical records).

Keep all papers with PHI (minimize) out of view of the public and dispose of properly (clinic sign in sheets).

Always use a fax coversheet.

Providence

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!

Providence

It’s Not Just PHI

In addition to PHI, you are expected to protect **Confidential Information,** which includes:

- 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

Removing confidential information requires supervisor/manager approval.

Be aware of security configurations in repositories.

Texting Guidelines

Do not text PHI. Utilize approved communication methods (Teams, Outlook, Epic In basket).

If you must text in an emergency situation, request a phone call back or keep it generic.

If you receive confidential information on your cell phone report it but do not share it.

Centers for Medicare and Medicaid Services (CMS) does not permit the texting of orders by physicians or other health care providers

Providence

Responsible Use of Social Media

Never use personal devices to take photos or record in patient care areas. A doctor using a personal device in a patient care area to capture images that seemingly do not identify a patient is still a violation of policy.   If you see others doing this report it immediately!

Never post textual descriptions of anything related to the care or treatment of a patient on your personal social media account. A unique story that you think is de-identified may be identifiable to a patient or their family. Marketing or Communications must review and approve all intended disclosures of patient information outside of Providence. Verbal permission is not sufficient.

Never share confidential or proprietary information about Providence or other workforce members even when your account is set to private. 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.

Providence

Media Requests

- If contacted by a reporter or the media about a patient, you should notify a Providence core leader or the house supervisor (politely declining requests for information).

- Only designated individuals within Providence are authorized as public spokespeople to speak with the media.

- The media should never be permitted within patient care areas and are treated as general visitors to the hospital (unless appropriately authorized by senior leadership) and appropriate patient consents and authorizations are in place.

Cyber Security at Providence

- 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.
- Personal device use must comply with all security policies (password protected, updated Operating System, patches, anti-virus, etc.) and the Use of Personal Device HR policy.
- Personal devices that contain Providence applications, programs, and apps are not to be used by anyone else or shared with anyone else.
- Any attempt to circumvent Providence security controls or non-compliance with policies can result in disciplinary action up to including termination of contract/partnership.

Personal devices include:

- *Smartphones*
- *Tablets*
- *iPads*
- *Desktop Computers*
- *Laptops*
- *Printers*
- *Gaming Devices*

Cyber Security Best Practices

- Keep all passwords private and secure. Do not share with anyone, **ever**!
- Lock or log off your computer when you walk away.
- Texting is not secure. If you must text PHI in an emergency, only provide the *minimum necessary*.
    - Centers for Medicaid and Medicare Services (CMS) has stated that physicians cannot create/share patient orders over text message, even in an emergency.
- To avoid phishing schemes, work related or personal, do no click on suspicious links or download attachments from unfamiliar senders, especially from email addresses you've never encountered before.

Completion Attestation

[illegible]

[illegible]

[illegible]

Providence

Providence

CME Evaluation and Claiming Credit

In order to obtain your credits/certificate for this Swedish CME activity, you will need to complete the course evaluation using the web address or QR code below. The final page of the evaluation will have a link to claim your credit.

https://forms.office.com/r/e9MDwJrWnQ

The maximum number of credit hours for this activity is 0.75. Your certificate will auto-populate after you submit your hours. Print, email or save your certificate *(you may need to have pop-ups enabled on your browser).*

Questions? Email cme@swedish.org

Providence SWEDISH

□han□you□

Confidentiality Policy

Department: Human Resources
Approved by: Chief Human Resources Officer
Date Last Reviewed: 10/25/2024
Date Last Revised: 9/21/2023
Date Adopted: 7/12/2019

Policy Name: Confidentiality

Scope: This policy applies to all workforce members.

Purpose: To provide guidance and direction with respect to the management, use and disclosure of confidential data/information.

Terms:

Workforce member means caregivers, volunteers, trainees, interns, medical staff, students, independent contractors, vendors and other individuals working at the ministry, whether or not they are paid by or under the direct control of the ministry.

Confidential data/information for purposes of this policy shall be any information, regardless of format, about patients, workforce members, or ministry operations that the ministry deems should not be available without specific authorization. Loss or inappropriate access to this kind of data could harm our patients, our ministry and our workforce. Confidential data/information includes, but is not limited to:

- Protected Health Information (PHI), electronic PHI, medical records, personally identifiable information including social security numbers, card holder data and financial information.
- Personnel records that the workforce member has chosen not to share (e.g., background checks records, drug test results, individual schedules, wages and similar information);
- Any privileged information from internal/external counsel;
- Any board, board committee or medical staff committee minutes or notes;
- Trade secrets or other confidential data/information or processes used by the ministry in carrying out its activities; and
- Any other data/information the ministry has deemed confidential.

Policy: Ensuring the protection of confidential, sensitive, and proprietary information is of critical importance to our workforce members, our patients, and the ministry. In keeping with our mission and values, the ministry requires workforce members to follow all policies, procedures and the Code of Conduct regarding use and disclosure of confidential data/information, and shall not purposefully access or disclose any confidential information unless (i) authorized to do so by the ministry; (ii) the confidential data/information is required to be disclosed to appropriate workforce members or employees of partner organizations to enable them to fulfill a legitimate job responsibility, provided the individuals receiving the information are advised of the confidential nature of the disclosure; or (iii) disclosure is required under applicable law. This policy is not intended to restrict workforce members from discussion, transmission or disclosure of wages, hours and working conditions in accordance with applicable federal and state laws.

Procedures:

Workforce members shall act with all reasonable and due care to avoid the inappropriate disclosure of any confidential data/information, including assuring that confidential data/information is maintained in secure files and locations, securely and appropriately handled, and stored and retained consistent with our guidelines and/or applicable law. Workforce members are prohibited from using confidential information for any personal gain or for the advantage of any outside organizations or entities. During the onboarding process, workforce members are required to sign a Confidentiality and Nondisclosure Statement. Selected covered persons may be required to sign additional and specific confidentiality statements or agreements if they are provided access to particularly sensitive confidential information. In addition, workforce members:

1. Will follow ministry policies and procedures and the Code of Conduct, and will take all precautions to prevent any intentional or unintentional use or disclosure of patient health information without the signed authorization of the patient.
2. Will only use and disclose that patient information that is minimally necessary in order to accomplish the intended purpose of the use or disclosure.
3. May not disclose that data/information unless directed by the ministry if their job function involves access to confidential wage and payroll information.
4. Will follow ministry policies and procedures and the Code of Conduct, and take all precautions to prevent any intentional or unintentional use, or disclosure of any trade secrets or confidential data/information about the ministry, its workforce members, and its programs.
5. Will follow ministry policies and procedures, and the Code of Conduct relating to complying with physical, technical, and administrative safeguards that are applicable to their work areas and scope of duties (i.e., use of encryption to send external email).
6. Will not use their access to patient health information, areas containing such information, and confidential data/information for purposes other than those necessary to perform their job functions.
7. Will not share access passwords to computer terminals and locked areas within the ministry, nor will workforce members use their unique usernames and passwords to allow access to other individuals, even if those individuals are authorized to access the data/information.
8. Will refrain from discussing patient care matters in inappropriate areas and other places deemed to be public areas (i.e., elevators, cafeterias, etc.).
9. Will complete all required privacy training.
10. Will cooperate in investigations.
11. Will immediately report instances of unlawful or inappropriate use, or disclosure of ministry or patient information to their core leaders, human resources, local privacy officer or through the Integrity Hotline and/or Integrity online, our web based reportion option – and will not be retaliated against for doing so, and may do so anonymously.
12. May be subject to corrective action up to and including termination for serious violations of policies related to use or disclosure of confidential data/information including but not limited to:
    A. Viewing of PHI (including demographic information alone) by use of identity look up modules in the electronic health record, or by use of other means, for the purpose of personal benefit/curiosity or when there is no business or medical purpose.
    B. Sharing confidential data/information or any other data created, owned or managed by the facility with external artificial intelligence chatbots.

References: Confidentiality and Nondisclosure Statement

Help: For questions about this policy, or assistance with understanding your obligations under this policy, please contact human resources or Region Compliance, Local Privacy Officer or the Region Compliance Director.

The statements of this policy document are not to be construed as a contract or covenant of employment. They are not promises of specific treatment in specific situations and are subject to change at the sole discretion of the ministry.