Status **Active** PolicyStat ID **9985853**

Implementation	06/2021
Last Reviewed	06/2021
Effective	06/2021
Last Revised	06/2021
Next Review	06/2026

Owner	David Lane: Chief Compliance Officer
Policy Area	Compliance
Applicability	Providence Systemwide + PGC

PSJH-RIS-734 Privacy Sanctions Policy

Executive Sponsor:	Sheryl Vacca, SVP, Chief Risk Officer
Policy Owner:	David Lane, VP, Chief Compliance Officer
Contact Person:	Cambria Haydon, Chief Privacy Officer

Scope:

This policy applies to 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.

☑ 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 Council with final approval by the President, Chief Executive Officer or appropriate delegate.

Purpose:

The Health Insurance Portability and Accountability Act (HIPAA) requires Providence to establish and apply appropriate Sanctions for workforce members who fail to comply with privacy regulations or privacy policies and procedures. This policy establishes violation levels to which Sanctions may be imposed by core leaders in collaboration with Human Resources and Risk and Integrity Services (RIS).

Definitions:

1. ***Protected Health Information (PHI)*** is any information, including demographic information, that

is created or received by Providence and relates to:

a. The past, present, or future physical or mental health condition of an individual;

b. The provision of health care to an individual;

c. The past, present, or future payment for the provision of health care to an individual; and that identifies the individual or for which there is a reasonable basis to believe the information can be used to identify the individual. PHI includes information concerning persons living or deceased (less than 50 years) and may be written, oral, or electronic.

2. ***Sanctions*** are disciplinary measures that may be imposed upon workforce members. Sanctions may include counseling, verbal or written warnings, or termination from employment as determined by the core leader in conjunction with HR and RIS. (see HR policies available on the HR Portal).
3. ***Privacy Violation*** means a failure to comply with, or follow, related state or federal privacy regulations or applicable Providence policies and procedures.
4. ***Use*** means the access or viewing of PHI.

Policy:

Workforce members who commit a Privacy Violation will be investigated and recommended for Sanctions based on the determination of level of the violation. The level of violation will be determined according to the severity of the violation, whether the violation was intentional or unintentional, the impact/influence of the event on the patient, the risk impact to Providence, and whether the violation indicates a pattern or practice of violations.

Sanctions will be applied based on the level of violation. Other mitigating and escalating factors *may* be considered as determined by the core leader in conjunction with HR and RIS. Any Sanction imposed on workforce members will be in accordance with the Levels of Violation (below) and applicable HR policies.

1. Levels of Violations:

A. **Level One** – Unintentional Violation: A violation will be classified as a Level One when it results from a situation where a workforce member was not expected to have knowledge on a certain topic, or the policy violation results from unintentional human error, and the workforce member has not had any previous Level One violations. Generally, a level one violation is a first or one-time occurrence.

B. **Level Two** – Intentional Violation: A violation will be classified as Level Two when it is deemed of low to moderate risk and results from a situation where a workforce member knew, or reasonably should have known, the practice or action is in violation of policy. A Level Two violation also may result when a workforce member repeats a Level One violation after being made aware of the policy requirements. Level Two violations include but are not limited to the following:

- Failure to secure credentials or workstation and/or sharing of credentials resulting in probable unauthorized credential use (including the unauthorized viewing of demographic information alone) by known or

unknown individuals.

C. Escalating and Mitigating factors that impact sanctions for Level One and Level Two Violations may include the following:

D.

Escalating Factors	Mitigating Factors
• Nature, severity, and frequency • Relationship of offense to workforce member's position • Prior disciplinary history • Brief period of time since the last violation • Pattern of similar violations Number of total violations • Evidence that the violation was grossly negligent • Impact to Providence operations, workforce clients, persons served • Impact to health and safety of workforce, clients, persons serviced	• Significant period of time since last violation • Technical or inadvertent error • No prior disciplinary history • No pattern of similar offenses • No evidence that the violation was grossly negligent • Systemic issues resulting in impossibility to comply with policy • Minimal impact to Providence operations, workforce, clients, persons served • The potential for re-education

E. **Level Three** – Intentional Violation: A violation will be classified as Level Three when it is deemed of significant risk and is the result of a deliberate action by a workforce member where the workforce member knew, or reasonably should have known, that the practice or action is a violation of Providence privacy and/or security policies**.** A Level Three violation also may result when a workforce member repeats a Level One or Level Two violation after being made aware of the policy requirements. Level Three violations include, but are not limited to, the following*:*
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 privacy/curiosity or when there is no business or medical purpose.
Level Three violations may be a first or one-time occurrence. Generally, mitigating factors will not be considered for Level Three violations

2. Sanction Exemptions:
Investigations of accesses, uses, or disclosures made by workforce members who are acting as whistleblowers or are victims of a crime may be exempt from Sanction application. Examples include but are not limited to a workforce member acting in good faith who:

- Believes that a workforce member has engaged in conduct that is unlawful or

otherwise violates professional or clinical standards; or believes that the care, services, and conditions potentially endanger one or more patients, workforce members, or other members of the general public.

- Discloses PHI to a federal or state health oversight agency or public health authority authorized by law to oversee the relevant conduct or conditions of Providence.
- Discloses PHI to an appropriate healthcare accreditation organization for the purpose of reporting the allegation of failure to meet professional standards of misconduct by Providence.
- Discloses PHI to an attorney retained by or on behalf of the workforce member for the purpose of determining legal options regarding disclosure conduct.
- Discloses PHI to law enforcement about the suspected perpetrator of a criminal act committed against a workforce member that is limited to the identification and location elements.

3. Retaliation:
   Providence will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against workforce members who:
   - File a complaint with Providence
   - Exercise their rights or participates in the Providence investigations process
   - File a complaint with the Secretary of Health and Human Services
   - Testify, assist, or participate in an investigation, compliance review, proceeding, or hearing
   - Oppose any act or practice that is unlawful under state or federal regulations, including HIPAA, providing that the individual acted in good faith, believing that the practice was unlawful, the manner of opposition was reasonable, and did not involve disclosure of PHI in violation of privacy regulations
4. Roles of the offices of the Chief Privacy Officer and the Chief Information Security Officer in application of Sanctions:
   The roles of the offices of the Chief Privacy Officer and the Chief Information Security Officer are to investigate and determine validity of reported violations, including assessment and assignment of violation level as applicable, and provide reporting and recommendation to management and Human Resources.
5. Retention of Sanctions documentation:
   Refer to PSJH-RIS-715 Records Retention and Disposal Policy.

References:

PSJH-RIS-722 Code of Conduct Policy
45 CFR 164.530 (e)(1)(2) 45 CFR 164.502(j) 45 CFR 164.512(f)(2)(l) 42 CFR Part 2

Please refer to the HR Counseling and Corrective Action policy and the Confidentiality policy, available on the HR Portal.

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
PSJH President/CEO	Cynthia Johnston: Sr Compliance Spec PSJH	06/2021
PSJH Executive Council	Cynthia Johnston: Sr Compliance Spec PSJH	06/2021
PSJH Policy Advisory Committee	Cynthia Johnston: Sr Compliance Spec PSJH	06/2021

Standards

No standards are associated with this document