KB0051071

Confidentiality Policy

Providence Milwaukie Hospital ("facility")

Department: Human Resources
Approved by: Chief Human Resources Officer
Date Last Reviewed: 9/21/2023
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 facility, whether or not they are paid by or under the direct control of the facility.

Confidential data/information for purposes of this policy shall be any information, regardless of format, about patients, workforce members, or facility operations that the facility deems should not be available without specific authorization. Loss or inappropriate access to this kind of data could harm our patients, our facility 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 check 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 facility in carrying out its activities; and
- Any other data/information the facility 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 facility. In keeping with our mission and values, the facility 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 facility; (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 facility 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 facility if their job function involves access to confidential wage and payroll information.
4. Will follow facility 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 facility, its workforce members, and its programs.
5. Will follow facility 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 facility, 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 facility or patient information to their core leaders, human resources, local privacy officer or through the Integrity Hotline and/or Integrity Online, our web based reporting 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 of 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 RIS 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 facility.

This policy does not modify the express terms of any collective bargaining agreement. In the event of a conflict between this policy and the terms of a collective bargaining agreement, the collective bargaining agreement will prevail.