

MAINE MEDICAL CENTER CONFIDENTIALITY AGREEMENT

This Confidentiality Agreement applies to Maine Medical Center [hereinafter referred to as “Entity”] employees, members of the Medical Staff, house staff, clinical affiliates, adjunct professional nurses appointed by the Department of Nursing, individuals authorized by the Chief Information Officer/VP of Information Services or designee, and others with business or patient care responsibilities at Entity *hereinafter collectively referred to as “users”*, who may have direct access¹ to patient, business, proprietary, trade secret, financial, human resource or other confidential communications, data and information systems of Entity, of MaineHealth, and/or of MaineHealth Member Organizations *hereinafter collectively referred to as “Organizations”* to perform their work-related obligations.

Users shall maintain the confidentiality, security and integrity of all information systems and of all patient, business, proprietary, trade secret, financial, human resource or other confidential communications and/or data of Organizations whether maintained in verbal, written, digital or electronic form. Users shall maintain the confidentiality, security and integrity of, and users shall not disclose, discuss, or enable access to, any confidential communications, data, or information systems of Organizations in any manner not consistent with the user’s job responsibilities and the terms of this Agreement, unless such actions are permitted as a matter of law.

I. General Confidentiality Principles.

User understands and agrees:

- The performance of their job or duties may require them to become aware of confidential information, which shall remain confidential consistent with the user’s work-related responsibilities and/or consistent with disclosures allowed by law. Confidential information includes:
 - Any patient information, including health care and financial information.
 - Employee personnel, compensation and health care information.
 - Business information relating to financial, administrative, and other information.
- Approval to access confidential information is a privilege that may be granted to the user based only on the responsibilities of their job or duties and that meets the need-to-know criteria for such access.
- The importance and obligations of patient confidentiality include:
 - Never discussing a patient’s case or presence outside of work, either with the patient, or with family or friends.
 - Never sharing password or system access codes.
 - Disposing of confidential information using Entity’s confidential destruction system.

II. Information Systems Access.

User understands and agrees:

- All network and software application passwords are confidential and shall not be disclosed to any third party including other authorized users of Organizations’ information systems.
- Access will be provided to them by uniquely assigned network and software application passwords necessary for access to Organizations’ computer networks and certain system and software applications appropriate for the user’s job function in their organization.
- Access to Organizations’ computer networks and software applications may include, without limitation, on-site access at the Organizations’ locations, remote access to defined systems or applications, or access through dedicated communications lines as appropriate.
- Network and software application passwords shall expire on a periodic basis and, upon the request of Entity’s Information Services; user shall be responsible for providing new, confidential passwords to continue to access Organizations’ computer network and software applications. Such passwords shall meet standards for length and content as may be modified from time to time.
- In the event that user reasonably suspects or becomes aware of any unauthorized use or disclosure of user’s network and software application passwords or other confidential user identification, user must immediately change such password or other user identification, and report such unauthorized use or disclosure to their organization’s Information Security Officer or designee, or Entity’s Audit and Compliance Department.
- Entity shall have the right to suspend or revoke user’s network and software application passwords without notice in the event of any breach or suspected breach of confidentiality or security.

¹ Direct access includes access to clinical, financial, management, operational, human resources, and other information systems of the Entity, of MaineHealth and/or of MaineHealth Member Organizations while onsite or via remote access.

III. Access to Electronic Medical Records, Related Clinical Databases and Systems.

User understands and agrees:

- To be accountable for all entries of patient information, orders and data entered by user into Organizations' information systems under user's network and software application password and electronic signature as applicable.
- To access patient information and/or records only for the following purposes in accordance with applicable state and federal laws and regulations: (i) providing health care to the patient or coordinating such care with other health care providers; (ii) billing and filing claims for reimbursement for care delivered to the patient; (iii) conducting scientific or statistical research, management or financial audits; (iv) conducting quality assurance, utilization review or peer review activities; (v) for technical support or remediation of network or software application functionality; and (vi) for database administrators' requirements involving verification and other operational purposes.
- To not disclose or re-disclose any patient information and/or records to any other entity or individual without the prior written authorization of the patient or the patient's authorized representative.
- To take appropriate security measures to prevent the unauthorized use of Organizations' information systems, software applications, network and data to which user has access.

IV. Access to Electronic Mail System and the Internet.

User understands and agrees:

- To access their Entity's E-mail System and/or Internet resources from Entity's network only for permitted purposes in accordance with Entity's applicable policies for such use.

V. Audits of Information Systems, Software Applications, Network and Data.

User understands and agrees:

- Entity may conduct unannounced audits of user's access to its information systems, software applications, network and data on a periodic basis to monitor appropriate use of and compliance with the obligations stated above.
- Any violation of patient confidentiality and/or unauthorized disclosure of proprietary information may result in disciplinary action, suspension or termination of clinical privileges and/or employment by Entity or termination of the business relationship with Entity as applicable. User also may be subject to legal action.

Signature

Printed Name

Date