**MAINEHEALTH CONFIDENTIALITY AGREEMENT**

This **Confidentiality Agreement** applies to the individuals (referred to as "Users") at MaineHealth Services or any of its subsidiaries (referred to as "Organizations") who may have direct access to patient, business, proprietary, trade secret, financial, employee or other confidential communications or data (referred to as "Confidential Information") and information systems of Organizations to perform their work responsibilities and includes:

1. Employees;
2. Medical Staff;
3. Housestaff;
4. Clinical Affiliates;
5. Adjunct Professional Nurses appointed by the Department of Nursing;
6. Clinical Researchers;
7. Individuals authorized by the CIO/SVP of Information Services or designee; and
8. Others with business or patient care responsibilities or contractual obligations.

**I. General Confidentiality Principles- User understands and agrees:**

- Performance of his or her work responsibilities may require User to become aware of Confidential Information, which shall remain confidential consistent with the User's work responsibilities, Organizations' policies and procedures, and disclosures permitted by law.
- Approval to access Confidential Information is a privilege that may be granted to the User based only on his or her work responsibilities and which meets the Organizations' need-to-know criteria for such access.
- To maintain the privacy, security and integrity of all Confidential Information and information systems of Organizations whether maintained in verbal, written, digital or electronic form.
- The duties relating to Confidential Information include:
  - Never discussing a patient's case or presence outside of work, either with the patient, or with family or friends.
  - Never posting any patient information or images on social media unless specifically authorized by the Organization and have obtained the appropriate patient authorization in advance.
  - Never sharing password or system access codes;
  - Never disclosing, discussing, or enabling access to any Confidential Information or information systems of Organizations in any manner unless such action is consistent with the User's work responsibilities, Organizations' policies and procedures, the terms of this Agreement and permitted as a matter of law; and
  - Never discussing any Confidential Information outside of work and ensuring that the disposal of such Confidential Information always occurs through the Organizations' confidential destruction system.

**II. Information Systems Access- User understands and agrees:**

- All network and software application passwords are confidential and shall not be shared with any third party including other authorized Users of Organizations' information systems.
- Access to Organizations' computer networks and certain system and software applications appropriate for the User's work responsibilities within his or her Organization(s), shall be provided with uniquely assigned network and software application passwords.
- Access to Organizations' computer networks and software applications may include, without limitation:
  1. On-site access at the Organizations' locations;
  2. Remote access to defined systems or applications; or
  3. Access through dedicated communications lines.
- Network and software application passwords expire on a periodic basis and, if requested by Organizations' Information Services Department, User shall provide new, confidential passwords for continued access to Organizations' computer network and software applications. Such passwords shall meet standards as may be mandated by Organizations from time to time.
- In the event that User suspects or becomes aware of any unauthorized use or disclosure of User's network and software application passwords or other confidential User identification, User immediately shall:
  1. Change such password or other User identification; and
  2. Immediately report any unauthorized use or disclosure to his or her Organization's Information Security Officer or designee, or the MaineHealth Audit and Compliance Department.
- Organizations have the right to suspend or revoke User's network and software application passwords without notice if there is any breach or suspected breach of the confidentiality or security of information systems access.

**III. Access to Electronic Health Records, Related Clinical and Research 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 linked to 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 state and federal laws and regulations:
    1. Providing health care to the patient or coordinating such care with other health care providers;
    2. Billing and filing claims for reimbursement for care delivered to the patient;
    3. Conducting scientific or statistical research;
    4. Performing management or financial audits;
    5. Conducting quality assurance, utilization review or peer review activities;
    6. Providing technical support or remediation of network or software application functionality;
    7. Performing database administrators' required functions involving verification and other operational purposes; and
    8. Sharing for legal or consultant 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, or in accordance with law, a statutorily authorized subpoena or a court order.
- To take appropriate security measures to prevent the unauthorized use of Organizations' information systems, software applications, network and data to which User has access including:
    - Securing hard copy documentation;
    - Locking or logging out of any information system when not in use; and
    - Concealing screens in use by turning them away from unauthorized viewers or using privacy screens where available.
- To access User's own electronic health records only through the Organizations' patient portals (*e.g*., MyChart).

**IV. Access to Information Systems Requiring Biometric Authentication- User understands and agrees:**

- Organizations collect, retain, and use certain biometric data (*e.g*., fingerprints, facial recognition, retinal scan) solely for purposes of identification and fraud prevention in connection with employee access to certain clinical and business information systems and software applications.
- Organizations shall use a commercially reasonable standard of care to store, transmit and protect from disclosure any paper or electronic biometric data collected from employees.
- Organizations shall not disclose or disseminate any biometric data to any third parties other than its attorneys, auditors and business associates except as follows: (i) obtaining the prior written consent to such disclosure or dissemination; (ii) disclosure is required by state or federal law or municipal ordinance; or (iii) disclosure is required pursuant to a valid search warrant, subpoena or court order issued by a court of competent jurisdiction.
- In the event that Organizations loan employees an iPad, cell phone or other mobile device which offers users the option of facial recognition or fingerprint authentication, then employees understand that they are responsible for deleting this biometric information prior to returning the device since such biometric data is stored locally on the device.
- User hereby consents to the collection and use of biometric data necessary to access certain clinical and business information systems and software applications of the Organizations.

**V. Access to Electronic Mail System and the Internet- User understands and agrees:**

- To access Organization's e-mail system and/or Internet resources from Organization's network only for permitted purposes in accordance with Organization's policies and procedures for such use.

**VI. Audits of Information Systems, Software Applications, Network and Data- User understands and agrees:**

- Organizations may audit User's access to its Internet resources, information systems, software applications, network and data on a routine basis without notice. This is to monitor appropriate use of and compliance with the obligations stated in this Confidentiality Agreement.
- Any unauthorized disclosure of Confidential Information may result in User being subject to one or more of the following as applicable:
    1. Disciplinary action including termination of employment
    2. Suspension or termination of clinical privileges
    3. Termination of the business relationship with Organizations
    4. Legal action

_____ _____ _____

Junior Volunteer Signature Printed Name Date

Maine Medical Center
MaineHealth

# Junior Volunteer Program
# Parental Consent and Media Release

In order for your child to become a volunteer with us, we need your consent and involvement in helping them have a productive and successful experience.

We ask that you assist your child by trying to avoid other commitments on their assigned volunteer day. This would include such things as driver's education, appointments, sports and work schedules. The Junior Volunteer program depends on a specific number of volunteers to be available each day so we can fulfill our service commitments to the hospital departments.

We understand there may be a time your child may not be able to come due to an illness, emergency or family vacation. Be sure to read the Junior Volunteer Guidelines for important information regarding attendance. Please note:

- Your child is **required** to attend his/her assignment during the first week of the program June 27 – July 1. There will be no excused absences during this week.
- Junior Volunteers **must complete** 7 of 8 days by the conclusion of the program on August 19, 2022.
- If your child is sick and needs to be absent from his or her volunteer assignment, s/he or you must call Volunteer Services by 8:15 AM to report the absence.
- If your child will miss a session for vacation, please let us know as far in advance as possible.

Orientation is mandatory for all new and returning Junior Volunteers.

- New Junior Volunteer Orientation on Tuesday, June 14th, 2022 from 3:30 – 5:30 PM
- Returning Junior Volunteer Orientation on Wednesday, June 15th, 2022 from 3:30 – 5:30 PM.

Placements in the program are contingent on attendance at Orientation, no exceptions.

**Parental Consent:**

I understand that my child, (name) _____ , wishes to participate in the Junior Volunteer Program at Maine Medical Center and I give my permission for him/her to serve in that capacity if accepted into the program. I understand that they will be expected to meet all the requirements of the position, including regular attendance and adherence to hospital policies and procedures. I have read and understand the material in the Junior Volunteer Guidelines and am aware of what is required of my son/daughter.

**Media Release:**

The undersigned authorizes Maine Medical Center and the Volunteer Services Department to use photographs, prints, negatives and reproductions of the above-named student for publicity, promotion, advertising, public relations, grant writing, or related purposes to further the aims and objectives of Maine Medical Center and/or the Volunteer Services Department.

Parent or Guardian Name (Print): _____

Relationship to volunteer applicant: _____

Signature of Parent / Legal Guardian: _____ Date: _____

***This form must include handwritten signatures. Electronic signatures are not acceptable.***