EMHS CONFIDENTIALITY AND INFORMATION SECURITY AGREEMENT AND ACCEPTABLE USE AGREEMENT (Consolidated)

Purpose: The Health Insurance Portability and Accountability Act (HIPAA) , the Health Information Technology for Economic and Clinical Health Act (HITECH) and other federal and state laws and regulations were established to protect the confidentiality of medical and personal information, and provide, generally, that patient information may not be disclosed except as permitted by law or unless authorized by the patient. These privacy laws apply to all members of the workforce. All EMHS workforce members are required to agree to and sign this agreement.

CONFIDENTIALITY STATEMENT

As an EMHS workforce member, I understand I may be working with confidential patient health and other sensitive information. This information may include, but is not limited to, medical records, personnel information, financial information, proprietary business information regardless of whether such information is communicated electronically, verbally, graphically or on paper.

I understand and acknowledge that under HIPAA I am required to receive education on privacy and security regulations and organizational policies, procedures and directives relating to the protection of health information. I agree to obtain all required education before I access, use, or disclose any patient information.

I acknowledge it is my responsibility to respect and protect the privacy and confidentiality of patient and other sensitive information. I will not access, use, or disclose patient or other confidential information unless I do so in the course and scope of fulfilling my duties as an EMHS workforce member. I understand that I am required to report immediately any information about the unauthorized access, use, or disclosure of patient information. Initial reports go to my supervisor and to the Privacy Officer (Acadia 973-6010; ALI, AHS, Meridian, and Miller Drug 973-7649; Beacon 973-4612; BHMH 374-3919 x3890; CA Dean 695-5265; EMMC Compliance Officer, 973-8551; EMHS Compliance Officer, 973-5100; Inland 861-3385; Lakewood 873-5125; MCMH 664-5962; Mercy Hospital 553-6114; Rosscare 973-7853; SVH 487-4022; TAMC 768-4280; VNA HHH 275-2128; and EMHS Information Security, 973-5948). If electronic media is involved, I will report the incident to the EMHS Help Desk at 207-973-7728 or 1-888-827-7728.

I understand and acknowledge that, should I breach any provision of this agreement, I may be subject to civil or criminal liability and/or corrective actions consistent with applicable EMHS and Member Organization policies and/or directives. For more information on HIPAA-related policies, procedures or directives, contact your supervisor.

Initial _____ Date_____

INFORMATION SECURITY ACCEPTABLE USE POLICY

Purpose: To establish requirements that all workforce members of EMHS and any other persons with access to EMHS information systems must follow to prevent the improper disclosure of confidential information and to prevent unauthorized persons from gaining access to confidential information. EMHS has a duty to safeguard confidential information available within its information systems and to ensure that any use of its computers, laptops and other electronic devices complies with federal and state laws and regulations, and organizational policies and directives.

Access: The information systems of EMHS are used to further the business and patient care objectives of EMHS and its members. This use is called “acceptable use.”

1. Access to EMHS organizational and patient information is permitted only according to approved policies and procedures.
2. All patient information on EMHS information systems are an extension of the medical record and are subject to approved policies and procedures governing patient medical records.
3. Only employees or approved agents of EMHS have access to business applications.
4. Other persons needing access must have a Data Access Agreement in place before being granted access to clinical applications.
5. Incidental personal use of information systems is permitted according to organizational policy and must not interfere with your work or the work of others.

6. Only the minimally necessary privileges or network services for the performance of assigned job tasks are allowed.
7. Security mechanisms that protect information systems may not be disabled or circumvented for any reason.
8. EMHS Information Security monitors access to EMHS information systems and systems use.

Initial _____Date_____

Passwords: Your password must meet EMHS standards for length and content.

Initial _____Date_____

Workstation Use: There are many ways in which network resources can be breached through an individual workstation.

1. Do not leave your workstation logged on in your absence. Lock your computer to protect it from unauthorized access. Turn your workstation off at the end of the day unless it is shared with another user.
2. EMHS Information Systems determines which hardware and software are installed on workstations and portable computers. Users must not install additional hardware or software without the permission of the System Administrator. This includes free software or shareware downloaded from the Internet.
3. Do not connect any device to the network without the approval of EMHS Information Security.
4. Report any suspected infection by malware to the EMHS Help Desk.
5. A deliberate introduction of malware onto an EMHS computer will result in corrective action up to and including termination for the user.
6. The use of this internet connection for the following activities is strictly prohibited:
    a. Spamming and Invasion of Privacy
    Sending of unsolicited bulk and/or commercial messages over the Internet using this connection or using it for activities that invade another's privacy.
    b. Intellectual Property Right Violations
    Engaging in any activity that infringes or misappropriates the intellectual property rights of others, including patents, copyrights, trademarks, service marks, trade secrets, or any other proprietary right of any party.
    c. Hacking
    Accessing illegally, or without authorization, computers, accounts, equipment or networks belonging to another party, or attempting to penetrate security measures of another system.
    d. Distribution of Internet Viruses, Trojan Horses, or Other Destructive Activities
    Distributing actual or information regarding Internet viruses, worms, Trojan Horses or denial of service attacks. Certain high bandwidth or potentially destructive protocols may not be available on this connection (e.g., bittorrent or p2p).
    e. Export Control Violations
    The transfer of technology, software, or other materials in violation of applicable export laws and regulations, including, but not limited to, the U.S. Export Administration Regulations and Executive Orders.
    f. Other Illegal Activities
    Using this connection in violation of applicable law and regulation, including, but not limited to, advertising, transmitting, or otherwise making available ponzi schemes, pyramid schemes, fraudulently charging credit cards, pirating or inappropriately distributing copy written material, or making fraudulent offers to sell or buy products, items, or services.
7. You understand that EMHS monitors all internet activity and you further understand that you should have no expectation of privacy whatsoever while visiting this connection.

Initial _____Date_____

Miscellaneous:

1. Patient information or protected health information (PHI) is any information related to the diagnosis, treatment or payment for healthcare that identifies the patient.
2. Patients have specific rights under Maine Law and HIPAA regarding their rights to privacy and confidentiality. These rights are outlined in our Notice of Privacy Practices.
3. Do not remove or send patient information or other confidential information outside the workplace without authorization.
4. Use an approved fax cover sheet containing the EMHS confidentiality notice with any outgoing fax.
5. Confidential information sent outside of EMHS by email must have "emhsecure" typed in the subject line of the message.
6. You may not access the medical record or account information of family members, dependents or any other individual, even if the person has signed a valid authorization giving you access or, if you are a legal guardian or personal representative, unless such access is necessary for patient care or to complete your assigned job duties. EMHS will not give you access to the electronic medical record just to look at your own record.
7. Documents containing confidential information must be disposed of in secure shredding bins. Magnetic media (disks, CDs, hard disks, backup tapes, etc.) must be disposed of in accordance EMHS policies and must be degaussed, shredded, or formatted to render them unusable for retrieving information.
8. Users must observe all intellectual property rights protected by copyright, patent, or trademark.
9. Users may not engage in communications that are threatening, defamatory, obscene, offensive or harassing.
10. Use of systems and other resources for political activity; illegal activities; gambling, or for personal gain or the gain of others for a non-EMHS purpose is prohibited.
11. Violations of this agreement and/or organizational policies relating to the protection of EMHS confidential information and the integrity of its information systems may result in a loss of access to information systems or to civil and criminal liability and/or corrective action consistent with applicable organizational policies.

Initial _____Date_____

Non-retaliation: EMHS will not permit retaliation for reporting a perceived or potential violation of the Code of Conduct, policies, laws or regulations including HIPAA or for participation in an investigation of any alleged violation.

_____	_____	_____
Employee Signature	**Printed Name**	**Date**

RETURN A COPY TO YOUR HUMAN RESOURCES DEPARTMENT. HR: RETAIN FOR DURATION OF EMPLOYMENT + 6 YEARS.