ENLOE HEALTH

November 2023

Subject: Access to Enloe Health Information Systems and Computer Applications

Dear Healthcare Provider, Business Associate or Vendor of Enloe Health:

Enloe Health (Enloe Medical Center) is committed to providing and promoting high quality health care to our patients and the community we serve. We are equally committed to: 1) safeguarding the integrity of our information systems and computer applications; and 2) ensuring the privacy and security of our patients' health information by relying on the HIPAA Privacy and Security Rules to govern our sharing of electronic health records.

Our records show that as a healthcare provider, current business associate or vendor of Enloe Health you and/or your employees currently have access to Enloe's information systems and computer applications, including our electronic health records, for the purposes of treatment, payment and/or health care operations. This access may include remote access.

Access privileges to Enloe Health's information systems and computer applications, including our patients' electronic health records, are granted for a period of one year, with an annual renewal prior to the end of each calendar year. Each individual granted access privileges is required to sign an *EMC Confidentiality of Information and Computer Access Agreement* when initial access is granted and annually thereafter.

This notice is being sent to you because it is time for the annual renewal of access privileges. If you or your employees have current access privileges or if you have employees who will need access, a new Agreement will need to be signed and emailed to Enloe Health Information Services at ISAdmin@enloe.org by December 31, 2023. If a signed agreement is not received by December 31st, the current access privileges will automatically be terminated.

If you have questions regarding the annual renewal process, please send an email to the email address noted above or call the Enloe HelpDesk at (530) 332-7899. Thank you for your cooperation and assistance in this matter.

Sincerely,

Susie Benson
Director, Safety/ Privacy Officer
Enloe Health
1531 Esplanade
Chico, CA 95926
(530) 332-5444

Enloe Health
Confidentiality of Information and Computer Access Agreement

Business Name:_____Phone:_____
Business Address Street: _____
City: _____ St.: _____ Zip: _____
Business Employee's First Name: _____ Last Name: _____
Email:_____ Job Title: _____
Home Address (Required for California residents) Street: _____
City: _____ St.: _____ Zip: _____

THIS CONFIDENTIALITY OF INFORMATION AND COMPUTER ACCESS AGREEMENT (herein-after "Agreement") is entered into with Enloe Health by the undersigned healthcare provider, business associate or vendor (herein-after known as "Business"), or by the undersigned employee of the Business (such person who is executing this Agreement being hereinafter referred to as the "undersigned"), effective as of the date set forth below the undersigned's signature.

BACKGROUND: Enloe Health has implemented a process whereby healthcare providers, business associates and vendors, and designated employees of such Businesses, for business purposes or for the purposes of treatment, payment and/or healthcare operations, can gain computer access to certain Enloe Health computer applications, internally and from remote locations, by logging onto Enloe Health's information systems and computer applications and entering a unique user ID code and password.

ACKNOWLEDGEMENT AND AGREEMENT: Enloe Health will assign to the undersigned a unique user ID code and password, which will allow the undersigned to access patient and/or other information through Enloe Health's information systems and computer applications. Each individual user ID code and password identifies each transaction the undersigned enters into the system, and as such identifies the individual as the legally responsible party for these transactions.

In consideration for such access, the undersigned acknowledges and agrees to the following:

1. ***As a Business with business relations with Enloe Health or any employee of such a Business, the undersigned has a duty to protect the confidentiality of patient information.*** Therefore, any patient information, if any, to which the undersigned is exposed within the course of his/her interactions with Enloe Health, including patient information accessed through the electronic health record system, shall be treated by the undersigned as highly confidential and shall not be disclosed to anyone other than the patient to whom such patient information pertains (or to patient's authorized representative) or persons having need of the patient information in order to perform professional duties respecting the patient. Patient information should not be accessed by anyone whose current professional duties do not require such access.

2. ***All requests for access, exchange, and use of Electronic Health Information (EHI), including Electronic Protected Health Information (ePHI), will follow Enloe Health policy. Enloe Health will provide EHI to valid requestors as defined and required under Office of the National Coordinator (ONC) and Centers for Medicare and Medicaid Services (CMS) Information Blocking provisions [45 CFR Parts 170 and 171].***

3. ***Enloe Health entrusts the undersigned to comply with the confidentiality requirements governing the use of patient information as defined by the California Confidentiality of Medical Information Act and the HIPAA Privacy and Security Rules.***

4. ***The undersigned will review and follow Enloe Health policies for Acceptable Use of Information Technology and Mobile Device Management.***

5. ***The undersigned will not disclose his/her ID code or password to anyone under any circumstance.*** The undersigned will not write or otherwise document his/her ID Code or password in any manner which would allow them to be viewed by other persons.

6. ***The undersigned is authorized to utilize Enloe Health's information systems and computer applications only in connection with the undersigned's business operations***. At no time shall the undersigned utilize Enloe Health's information systems and computer applications for any reason other than its intended use, which is to perform professional duties respecting the undersigned's business operations. Any actual or attempted access by the undersigned to information other than required by his/her business shall constitute a breach of this Agreement, for which Enloe Health may seek such legal redress and damages as may be allowable under applicable law. Additionally, any such breach shall subject the undersigned to revocation of the undersigned's privilege to utilize the information system.

7. ***When the undersigned logs onto and gains access to information through Enloe Health's computer information systems and computer applications, he/she will not allow any unauthorized person to view the information thereby accessed.*** Prior to leaving the physical vicinity of a PC or mobile device upon which he/she has logged onto Enloe Health's information systems and computer applications, the undersigned will ensure that he/she properly logs out of the system.

8. ***Use of the undersigned's user ID code or password by anyone other than the undersigned is forbidden under any circumstances.*** A Business shall not permit his/her employees or any other person to access Enloe Health's information systems and computer applications by using the Business ID code and password; rather, any access by a Business employee must be through each employee's own ID code and password. Only employees of a Business who are specifically designated by such Business shall be eligible to receive a user ID code and password. **Sharing of user ID codes and passwords is PROHIBITED.**

9. ***If the undersigned learns or has reason to believe that his/her user ID code or password may be known by others, the business or undersigned shall immediately notify Enloe Health's Helpdesk at (530) 332-7899 so that the suspect user ID/Password may be deleted and a new one issued. The business or undersigned shall also notify Enloe Health's Privacy Officer at (530) 332-5444 to ensure compliance with State law requiring the prompt reporting and investigation of privacy and security breaches.***

10. ***The undersigned will ensure that appropriate security measures are implemented and maintained respecting any PC or mobile device utilized by the undersigned to access Enloe Health's information systems and computer applications.*** Without limiting the generality of the preceding sentence, the undersigned agrees that, unless authorized by Enloe Health, he/she will not cause or permit any patient information to be electronically downloaded, saved or otherwise stored on any such PC or portable media and the undersigned will take all reasonable and practical measure to minimize the risk of unauthorized access to the electronic health record system through such PC or mobile device.

11. ***Any Business who requests a user ID and password for their employee shall have the responsibility to immediately notify Enloe Health's Information Services at ISAdmin@enloe.org or the Enloe HelpDesk at (530) 332-7899 in the event the employment of such employee is terminated*** or in the event of any other change in circumstances that would make such employee's continued access to Enloe Health's computer information system and applications inappropriate.

I acknowledge that I have read and agree to follow this Agreement. I understand that if I violate this Agreement, I will be subject to losing the privilege of access to the Enloe network and possible criminal and/or civil action. All transactions are logged and audited regularly.

Business Employee **Signature**: _____

Business Employee **Printed Name**: _____

Last 4 digits of Business Employee's **Social Security Number (REQUIRED)**:_____ **Date**: _____

Business Authorizing Party/Supervisor **Signature**: _____

Business Authorizing Party/Supervisor **Printed Name**: _____ **Date**: _____

INFORMATION SERVICES
ACCEPTABLE USE OF INFORMATION TECHNOLOGY POLICY

PURPOSE

The purpose of this policy is to establish management's commitment to a formal *Acceptable Use of Information Technology Policy* to protect the confidentiality, integrity, and availability (CIA) of patient health information, hospital data, and employee data as well as protect the infrastructure that supports our services and business activities. This policy aids Enloe Health (EH) in meeting its obligations with regard to information security and privacy. This policy has been designed to meet or exceed applicable federal and state regulatory obligations.

SCOPE

The scope of the *Acceptable Use of Information Technology Policy* extends to all functional areas and all employees, consultants, contractors, temporary staff, interns, partners, and third-party employees who access EH's information technology systems and information. The scope also extends to all computing devices used at EH: workstations, mobile devices, laptops, servers, software, and hardware, including medical devices.

POLICY

Producing, exchanging and retrieving information electronically through the use of computer technology and other forms of electronic communications presents valuable opportunities for EH. While staff are expected and encouraged to use this technology, its use carries important responsibilities.
Computer systems, telecommunications and electronic media equipment (including workstations, laptops, printers, wired and wireless networks, software, facsimile machines, electronic mail, Internet and Intranet browsing, telephone systems, and voice mail) are to be used in accordance with EH standards.

The use of information technology is a privilege extended by EH, which may be revised, restricted or withdrawn at any time. These technologies are EH property and are to be used solely for business purposes.

STANDARDS (General)

- Staff are responsible for protecting the passwords used to access EH computer systems and information. Sharing user identifications, passwords and account access codes or numbers is prohibited. Staff must make all efforts to safeguard this information from unauthorized users. Staff may be held responsible for misuse that occurs through such unauthorized access.

- Staff must not attempt to access information for which they are not authorized.

- EH provides a voice mail system, electronic mail system and network connections for internal and external business communication and data exchange purposes. Use and access of these systems may be filtered, monitored and tracked at any time. Even though files, data, or messages may appear to be deleted, procedures by EH to guard against data loss may preserve material for extended periods of time.

- The following items are prohibited from transmission on any electronic communication system:
    - Any item that is in conflict with EH's Preventing Discrimination, Harassment & Retaliation in the Workplace policy. For example, staff may not communicate messages that would constitute unlawful or sexual harassment, and may not use sexually offensive material or information, offensive screen savers, or access offensive web sites;
    - Any item that is in conflict with EH's Corporate Compliance Program and Employee Guide with Code of Conduct;
    - Commercial use that is in conflict with EH;
    - Use that violates trademark, copyright or license rights;
    - Participation either directly or indirectly in any gambling activity; or
    - Social Networking sites, unless explicitly authorized to do so.

- The use of EH provided Internet access is intended to be solely for business related purposes. Internet access is filtered and monitored and actual web-site connections are recorded.

- In order to ensure continuous access to information of EH systems, no staff shall use personal hardware or software to encrypt e-mail, voice mail or any other data stored in EH systems.

- Introducing or using software designed to monitor, destroy, or corrupt computer systems with viruses or cause other harmful effects is prohibited. Staff are required to use EH provided anti-virus technologies.

- It is the policy of EH to respect the proprietary rights of the companies who develop and support the computer software we use. All EH staff that use a computer system are required to comply with license agreements associated with the computer software products used. Staff may not use these systems for any purpose that violates the law. You must not make illegal copies, download or transmit information or software in violation of copyright laws. No software can be installed on any computer system without the prior written permission from the Chief Information Officer.

- All installed software must comply with standards approved for EH use.

- Staff are responsible for the computer equipment made available for their use and to follow established procedures to protect the equipment from loss or damage.

- Any mobile devices used for business purposes (cell phones, tablets, laptops), must have a PIN set to unlock the device. Ensure mobile devices are out of sight and secure when not in one's possession.

- Do not travel with EH mobile devices unless it is needed and do not put mobile devices in checked luggage.

- Unauthorized alteration or destruction of computer hardware, software, or data is not permitted.

- Network connectivity is allowed only under direction of Information Services. If an unauthorized device is connected to the network, the device will be disconnected and the staff member's management informed.

- Equipment issued to staff must be returned to EH upon separation from service. If it is not, the staff may be responsible to pay for replacement of the equipment, and EH may take legal action to collect same should the staff fail to return the equipment or make payment.

- It is important to exercise care when sending or receiving sensitive, privileged, proprietary, or confidential information. Communications must be identified as privileged and/or confidential when it is appropriate to do so.

- Staff will not send or receive confidential information when unauthorized persons may have visual access.

Staff will not access personal email accounts (gmail, etc) on Enloe workstations, Enloe mobile devices, or any other Enloe owned devices.

STANDARDS (E-mail)

- EH encourages the business use of e-mail to increase productivity. The e-mail system and all messages generated by or handled by e-mail, including backup copies, are part of the business assets of EH. E-mails are owned by EH and are not the property of the end users of the system.

- The e-mail system is only to be utilized by staff for the business use of EH. E-mail accounts will be available for all staff having a business need.

- Antivirus and antispam filtering technologies are employed for both inbound and outbound e-mail messages.

- E-mail users do not have a right to privacy. EH may monitor, audit, delete, and read e-mail messages to support operational, maintenance, auditing, privacy, information security, and investigative activities.

- E-mail use will not involve any illegal or unethical activity, or involve or disclose any activity that could adversely affect EH or its staff.

- Unique user-identifications and associated passwords will be employed when accessing e-mail. All e-mail containing electronic protected health information (ePHI) will contain

'confidential' in the subject line for encryption when sent to non-Enloe e-mail, ensuring compliance with the HIPAA Security Rule.

- Staff may not forward to anyone outside EH sensitive information, including ePHI that has not been encrypted**,** and without prior approval from the department manager.

- Forwarding and auto-forwarding of e-mail to non-Enloe email accounts is strictly prohibited.

STANDARDS (Remote Access)

- Remote access to EH systems or data may be permitted for conducting EH Business.

- Only authorized individuals will be granted remote access.

- The method of remote access permitted for an end user will be determined by and managed by Information Services. Remote access methods can vary and will depend on the purpose for access, the systems and data being accessed, the remote devices being used, and other factors including HIPAA security requirements.

- All end users are responsible to sign-off/disconnect/lock the workstation when leaving unattended such that no information is left visible and any returning end user is required to enter a password to gain access.

- Troubleshooting connection difficulties is the responsibility of the end user (based on defined steps from Information Services).

- It is considered misuse for staff to download any ePHI or confidential information to any remote device no matter what the platform, to include: tablets, mobile phones, laptops, remote storage devices, etc. without prior approval from the Chief Information Officer.

- Formal procedures must be followed to request or modify remote access.

- EH reserves the right to terminate remote access privileges for any reason.

STANDARDS (Hardware and Software Standards and Purchases)

- Information Services will use the purchasing power of our Group Purchasing Organization contract whenever possible.

- Computer hardware and software will be purchased per the current Information Services Department standards. Only approved software may be installed on computer systems purchased by EH.

- Software will not be purchased, installed, downloaded, copied or shared, except under the direction of Information Services. Installed software is owned by EH and managed by the Information Services Department.

- All contracts and purchase requisitions pertaining to computer hardware, software, services, and support agreements must be approved by Information Services.

- If non-approved software is found residing on a workstation owned by EH, the department manager responsible for the area housing the workstation will be notified and the software removed.

POLICY EXEMPTIONS

Where compliance is not technically feasible or justified by business needs, an exemption may be granted. Exemption requests must be submitted to the Helpdesk, including justification and benefits attributed to the exemption. The Risk Acceptance Request Process should be followed in accordance with the Risk Acceptance Request Procedure.

APPLICABILITY AND ENFORCEMENT

Failure to comply with this information security policy could damage both the reputation of the organization and impair its ability to achieve its goals. Non-compliance may result in disciplinary action up to and including termination of employment.

REFERENCE POLICIES AND PROCEDURES

Mobile Device Policy
User Account and Password Policy
Preventing Discrimination, Harassment & Retaliation in the Workplace Policy
Corporate Compliance Program and Employee Guide with Code of Conduct

REFERENCES

Health Information Portability and Accountability Act 45 CFR §164.308

INFORMATION SERVICES
MOBILE DEVICE MANAGEMENT (MDM) and PORTABLE STORAGE MEDIA POLICY

PURPOSE

The purpose of this policy is to establish management's commitment to a formal Mobile Device Management and Portable Storage Media Policy to protect the confidentiality, integrity, and availability (CIA) of client information, company data, and employee data as well as protect the infrastructure that supports our services and business activities. This policy aids Enloe Health (EH) in meeting its obligations with regard to information security and privacy. This policy has been designed to meet or exceed applicable federal and state regulatory obligations.

SCOPE

The scope of this policy extends to all functional areas and all employees, volunteers, consultants, contractors, temporary staff, interns, partners, and third-party employees who access EH's IT systems and information and allows EH to develop procedures to secure and audit its IT resources.

For the purposes of this policy, the following general definitions are applicable:

Mobile devices are electronic devices that can store, process and transmit/receive electronic data. Examples include but are not limited to:

- Laptops
- Tablets
- Smartphones
- Voice recorders
- Video and still cameras
- Smart Pens

Portable Storage Media is media that can be used to store and transport electronic data. Examples include but are not limited to:

- USB flash drives
- Flash memory devices such as Compact Flash and MicroSD cards
- External hard drives,
- Zip drives
- Data tapes
- CDs and DVDs
- Floppy disks

This policy applies to all mobile devices used at EH, which are used to conduct EH business, connect to EH networks, or access any Enloe systems. The policy is applicable to devices that are EH-owned or personally-owned, no matter where the device is located and applies to devices that contain sensitive EH data including ePHI as well as those that do not contain ePHI.

This policy allows EH to develop procedures to:

- establish usage guidelines
- require device encryption and remote wipe capabilities as appropriate
- guide implementations
- ensure appropriate responsibility and accountability
- prevent improper use
- disable non-compliant devices
- manage and support devices
- comply with the HIPAA Privacy and Security Rule

POLICY

EH-owned mobile devices will only be issued to individual employees who agree, as a condition of device usage, that their use of the device will conform to EH policies and procedures. EH-owned mobile devices will be uniquely identified and managed.

Non-EH issued mobile devices may be used for EH access and is granted by Information Services (IS) through formal procedures and the use of IS-approved remote access tools/methods. As a general rule, only exempt employees will be allowed to have remote access to EH. Any exceptions must be approved by the Human Resources Department.

Only encrypted portable storage media issued by EH may be used to connect to EH devices and systems. ePHI or other sensitive information shall not be saved to portable media unless expressly approved by the Information Security Manager or Risk & Compliance Manager.

Smartphones (EH-owned and personally-owned) used to access Enloe systems may be required to have Mobile Device Management (MDM) software installed.

Any loss or compromise of a mobile device or portable media must be reported to the Enloe Help Desk within four hours, who will report it to the Information Security Manager and Risk & Compliance Manager.

STANDARDS

- All EH laptops will be encrypted to the appropriate standard.
- MDM software will be used to remotely wipe Smartphones in the event of loss or theft.
- MDM software will force encryption on mobile devices connected to the EH network.
- A pin or passcode is required on all Smartphones connected to the EH network.
- A pin or passcode is required on all encrypted storage media.

POLICY EXEMPTIONS

Where compliance is not technically feasible or justified by business needs, an exemption may be granted. Exemption requests must be submitted to the Helpdesk, including justification and benefits attributed to the exemption. The Risk Acceptance Request Process should be followed in accordance with the Risk Acceptance Request Procedure.

Tapes and backup media are covered under Backup and Recovery procedures.

APPLICABILITY AND ENFORCEMENT

Failure to comply with this information security policy could damage both the reputation of the organization and impair its ability to achieve its goals. Non-compliance may result in disciplinary action up to and including termination of employment.

REFERENCE POLICIES AND PROCEDURES

Risk Acceptance Request Procedure
Mobile Device Procedure

REFERENCES

Health Information Portability and Accountability Act 45 CFR §164.308(a)(4)
NIST 800-66 Rev. 1 An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule