Healthy Driven
Edward-Elmhurst
HEALTH

Information Technology Code of Compliance

Employees of Edward-Elmhurst Health ("EEH"), EEH Medical Staff members and their Office Staff, and independent contractors of EEH (collectively "Users") who require access to EEH Technology Systems.

All Users who need access to EEH Information Systems must read this policy, abide by its requirements, acknowledge receipt and accept its terms by signing below. Each individual that requires access to an Information System including but not limited to: computer systems, voice mail systems and electronic mail systems (collectively "systems") must sign and return this document to EEH Human Resources ("HR") or their EEH Sponsor prior to obtaining permission to access the systems.

Levels of access will be granted as follows and may be modified or terminated by EEH at any time and/or for any reason in EEH's sole discretion:

1. **EEH employees** will be granted access based on their job functions and responsibilities and approved by the employee's manager; changes in access required by changes in responsibility shall be approved by the employee's manager;
2. **Medical Staff members** will be granted access based upon their need for access in the care and treatment of their patients;
3. **Office Staff** will be granted access based upon job functions and responsibilities and only for the Medical Staff member's patients; any such Office member must have the EEH Medical Staff Office approval for computer access (EEH Medical Staff Office approval designee's are maintained by the Access Security Team);
4. **Other non-employed individuals** may be granted access in accordance with the scope of duties and services to be performed under the terms of their contract. This access may be subject to a risk assessment and will require approval by the non-employee's responsible EEH manager (sponsor).
5. **Unmanaged Technology Resources** will be permitted access to on a case by case basis. Users requiring access to technology resources not provided by IT will be required to submit a request, approved by their supervisor or sponsor, including: the business need to the organization, and a signed copy of the Unmanaged Technology Usage Agreement ("UTUA") approved by the System Director of Technology or the Manager of Technology Security and Compliance.

Users must

1. Maintain the confidentiality of their access credentials (e.g., user name, password, access code, etc.);
   a. Not allow another person to use one's access credentials;
   b. Not use another person's access credentials;
   c. Not email passwords;
   d. Not give passwords over the phone.
   IT personnel will never ask for password information over the phone or in e-mail correspondence
2. Not access Protected Health Information (PHI) , Personally Identifiable Information (PII), or any EEH confidential information for any purpose other than in accordance with their scope of duties and job functions;
3. Not access any other individual's PHI other than your own record, or that of your minor child 11 or younger other than in accordance with their scope of duties and job functions;
4. Not e-mail *PHI/PII or business confidential information* unless using approved encryption methods;
5. Only use authorized portable devices with password protection and encryption enabled when working with PHI/PII or business confidential information;
   Encrypted USB Flash Drives can be obtained from the IT Service Desk upon request
6. Not save ePHI/ePII or other business confidential information on public, personal or unapproved network locations;
7. Report the following to the IT Service Desk immediately:
   a. Lost or stolen computing or mobile devices;
   b. Suspicious, unsolicited e-mails;
   Do not open
   c. Unknown media (CDs, flash drives, external hard drives, etc.).
   Do not connect them to your computer or the network
8. Not provide confidential information to anyone until you verify their identity and the reason for their request;
9. Log-off or lock your desktop computer when you leave it unattended to protect it from use by unauthorized persons;
10. Not remove privacy screens or similar privacy controls attached to devices;
11. Take care to protect confidential information from being viewed by onlookers;
12. Not hold secured doors open for unknown individuals without asking them to identify themselves;
13. Wear badge identification at all times while working;
14. Dispose of sensitive data in approved shred bins or through similar approved methods;
15. Not use EEH email for personal reasons, or a manner inconsistent with EEH values;
16. Not use auto-forwarding technologies to send EEH emails to a non-EEH email address;
17. Not send PHI or PII via text or other insecure messaging system;
18. Only use approved messaging applications for communicating PHI or PII on mobile devices.

Software

It is the standard of EEH to respect all computer software copyrights and to adhere to the terms of all software licenses.

1. Individuals may not duplicate any licensed software or related documentation for use within the corporation or elsewhere;
2. Only software acquired through Purchasing, authorized, and installed by Information Technology Services may be used on EEH computers;
3. Individuals are not permitted to load non-EEH owned software onto EEH owned devices;
4. Individuals are not permitted to load EEH owned software onto non-EEH owned devices;
5. Duplication/installation in violation of the software policy will subject employees to disciplinary action up to and including termination of employment;
6. Unauthorized duplication/installation by Medical Staff members or their Office Staff may result in the termination of their access to EEH Information Systems.

Hardware

It is the standard of EEH to track and protect all hardware assets at all times. By signing this agreement, you agree to adhere to all applicable EEH policies and standards as it relates to the use and configuration of any EEH owned device issued to you.

1. Assets are to be connected to the EEH network at least every 30 (thirty) days;

Electronic Signature

I acknowledge that my electronic signature will be used only by me to authenticate the part of the electronic medical record and/or other computer application/program that is my responsibility. I will not disclose my electronic signature credentials to any other person or permit another person to use it. I understand that patient information is confidential and agree to follow EEH's policies and standards for protection of sensitive information.

Acceptance

My signature constitutes my acceptance of the Edward - Elmhurst Health Information Technology Code of Compliance and that I will abide by all applicable EEH policies, standards and procedures applicable to EEH Information Systems (collectively "Information Technology Policies"). I further agree to maintain the privacy and confidentiality of health care information in accordance with applicable State and Federal laws , Health Insurance Portability and Accountability Act of 1996 (HIPAA), and HITECH.

I recognize that EEH monitors and audits my use of the Systems at all times. I agree to provide EEH with any documentation or information necessary for EEH to support such monitoring/auditing and to cooperate with EEH in performing such monitoring/auditing. I acknowledge that I have no expectations of privacy in regards to my use of EEH systems. I acknowledge that I am responsible for any and all actions executed with my User ID.

Violations of the EEH Information Technology Code of Compliance may result in the following:

1. Disciplinary action up to and including termination of employment or contract;
2. Medical Staff members or members of their Office Staff may be deprived of access to the Information Systems;
3. Independent contractors may be deprived of access to the Information Systems and their contract with EEH terminated.

EEH reserves the right to pursue any available legal remedies for such violations

Recipient

Name Printed: _____ Company: _____

Signature: _____ Department: _____

Date: _____ Title: _____