Edward-Elmhurst HEALTH | Healthy Driven

ACCESS SECURITY PROFILE FORM: NON- EMPLOYEE

Compliance Form Completed - Attached ☐

Have you ever done a student rotation, volunteered, or worked for Edward-Elmhurst Health? Yes or No

FULL NAME: _____ _____ _____
First *Middle* *Last*

COMPANY/
PRACTICE: _____

For providers and their staff please indicate both your company and if applicable the specific practice/location you are associated with

ADDRESS: _____ _____
Street *City, State, Zip-code*

Job Title: _____

Office Phone #: _____

Office Email: _____@_____

From selection below please **choose THREE** *questions below to answer. The questions you choose will be additional information that will be used to verify your identity by telephone when you contact technical support.

Q1: City of Birth **A.**_____

Q2: Address **A.**_____

Q3: Year of Graduation **A.**_____

Q4: Mother's Maiden Name **A.**_____

Q5: High School Attended **A.**_____

Q6: Day of Month you were born **A.**_____

*User Signature*_____ *Date*_____

Access Authorization

A Service Now request is created for each new Non-Employee user account access request. An Edward-Elmhurst Healthcare Manager or designee indicates authorization/approval through the Service Now request. This form should accompany that request in the system.

Exhibit D
Information Technology Code of Compliance

This **IT Code of Compliance** applies to Employees of Edward-Elmhurst Health ("EEH"), EEH Medical Staff members and their Office Staff, independent contractors of EEH, EEH authorized workforce, and authorized non-employee workforce, and any other approved Workforce who require access to EEH Technology Systems (collectively "Users").

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. Violations of this IT Code of Compliance are subject to disciplinary action in accordance with the EEH Privacy and Information Security Sanctions policy or termination of relationship.

Levels of access will be granted as follows and may be modified or terminated by EEH Information Security 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 Sponsor;

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 (a record of EEH Medical Staff Office approval designees and Sponsors are maintained by the Access Security Team);

4. **Other non-employed workforce** 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, Director, or 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 Sponsor, including: the business need to the organization, and a signed copy of the Unmanaged Technology Usage Agreement ("UTUA") approved by the Chief Information Security Officer, Associate Vice President, IT, System Director of Technology, or the Manager of Technology Security and Compliance. Termination of access is the Manager's responsibility as defined in EEH System Policy, Access Management, ITS-010.

Definitions

Sponsor – User's EEH Manager, or above.

Workforce - Employees, physicians, volunteers, trainees, students, and other persons whose conduct, in the performance of work for the System, is under the direct control of the System, whether or not they are paid for such work by the System.

PHI – Means any health information (including demographic information collected by the System from the individual pursuant to HIPAA), which is: (a) created or received by the System; (b) relates to the past, present, or future physical or mental health condition of an individual; (c) the provision of health care to an individual; (d) the past, present, or future payments for the provision of health care to an individual; and/or (e) identifies the individual or in which there is a reasonable basis to believe that the information can be used to identify an individual. PHI may take any form of media; including oral, written or electronic forms. It excludes health information contained in employment records held by the System in its role as employer. ePHI in an electronic version, copy or record of PHI.

PII - means any personal data or personal information (such as a social security #, driver's license #, or account #) pursuant to Illinois' Personal Information Protection Act (PIPA). ePII in an electronic version, copy or record of PII.

PCI – PCI is a subset of PII. The PCI Payment Card Industry Data Security Standard (PCI DSS) applies to all entities that store, process, and/or transmit cardholder data. It covers technical and operational practices for system components included in or connected to environments with cardholder data. If you accept or process payment cards, PCI DSS applies to you. (PCI Security Standards Organization). ePCI in an electronic version, copy or record of PCI. Passphrase – Complex password that meets EEH policy criteria as defined in the Identity and Access Management Standard, 011.

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 with proper ISS management authorization, installed by, or with approval from Information Technology Services may be used on EEH devices.
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; if there is a need, employee will need prior approval from EEH management.
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.

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, job functions and EEH policies;
3. Not e-mail PHI/PII or EEH business confidential information unless using approved encryption methods;
4. 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
5. Not save ePHI/ePII or other business confidential information on public, personal or unapproved network locations;
6. 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
7. Not provide confidential information to anyone until you verify their identity and the reason for their request;
8. Log-off or lock your desktop computer when you leave it unattended to protect it from use by unauthorized persons;
9. Not remove privacy screens or similar privacy controls attached to devices;
10. Take care to protect confidential information from being viewed by onlookers;
11. Not hold secured doors open for unknown individuals without asking them to identify themselves;
12. Wear badge identification at all times while working;
13. Be aware that personal use of EEH email and assets is not private and may be monitored or recorded by EEH.
14. Dispose of sensitive data in approved shred bins or through similar approved methods;
15. Not use EEH email address or credentials for non EEH applications or websites;
16. Not use auto-forwarding technologies to send EEH emails to a non-EEH email address;
17. Not send PHI or PII via unapproved or insecure text or other messaging systems;
18. Only use approved messaging applications for communicating PHI or PII on any device.

Hardware

It is the standard of EEH to track and protect all equipment and device 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.

IT Code of Compliance Attestation

Follow all EEH policies.

The main policy requirements are emphasized below but this may not be a complete list. Please refer to the EEH policy portal for all policy requirements.

A. Maintain the confidentiality of my access credentials (e.g., username, passphrase, access code, etc.):
   1. Not allow another person to use my access credentials
   2. Never share their passphrase and access credentials via any method, including verbally
   3. Not use another person's access credentials
   4. Not email passphrases ***IT personnel will never ask for passphrase information over the phone or in e-mail correspondence.***

B. Not access PHI/PII/PCI or any EEH classified record types for any purpose other than in accordance with my scope of duties and job functions, and EEH Standard Data Classification, 063;
C. Encrypt emails by typing SECURE in the subject line when sending any PHI/PII/PCI outside of the organization.
D. Not send PHI/PII/PCI to any personal email address without prior authorization.
E. Only use portable devices with passphrase protection and encryption enabled when working with PHI/PII/PCI or business confidential information.

Encrypted USB Flash Drives can be obtained from the IT Service Desk upon request

A. Not save PHI/PII/PCI, or other business confidential information on public, personal, social media, or unapproved network locations, including the EEH network folder named "Public (P)".
B. Report the following to the IT Service Desk immediately:
   1. Lost or stolen computing or mobile devices, including personal devices with any EEH system access.
   2. Suspicious, unsolicited e-mails; Do not open, and report as spam by forwarding to spam@eehealth.org
   3. Unknown media (CDs, flash drives, external hard drives, etc.). Do not connect them to your computer or the network

C. Log-off or lock my desktop computer when I leave it unattended to protect it from use by unauthorized persons. Any activity under your login is linked to your access credentials.
D. Not remove privacy screens or similar privacy controls attached to devices.
E. Take care to protect confidential information from being viewed by onlookers.
F. Not hold secured doors open for unknown individuals without asking them to identify themselves.
G. Wear badge identification at all times while working.
H. Be aware that personal use of EEH email and assets is not private and may be monitored or recorded by EEH.

Inappropriate or excessive use may result in disciplinary action, as determined by the user's Sponsor.

A. Not use EEH email address or credentials for non EEH applications or websites.
B. Not use auto-forwarding technologies to send EEH emails, or proprietary information to a non-EEH email address.
C. Not send PHI/PII/PCI via unapproved, unsecure text or other messaging systems, or social media.
D. Only use social media platforms on my EEH device within the scope of my position, and I must adhere to all terms in the Electronic and Social Media Policy, LGLRSK_004.
E. Only use approved messaging applications for communicating PHI/PII/PCI any device.
F. Monitor access activity on my EEH DUO accounts, and I must approve only authorized DUO access requests.
G. Must report any unusual activity on my EEH DUO account.

Name Printed: _____ Company Name: _____

Signature: _____ Department: _____

Date: _____ Title:_____