

## INFORMATION SYSTEMS CODE OF COMPLIANCE (p1 of 2)

### INFORMATION SYSTEMS SECURITY POLICY:

Employees of Edward Hospital and Health Services (“Edward”), Edward Hospital Medical Staff members and their Office Staff, and independent contractors of Edward frequently require access to Edward Information Systems (including but not limited to computer systems, voice mail systems and electronic mail systems). All Edward employees, Medical Staff members, Office Staff, and other non-employed individuals who need access to Edward’s Information Systems must review this policy, abide by its requirements, and acknowledge receipt and acceptance by signing below. Each individual who desires access to the Systems must sign this policy and return it to Edward prior to obtaining permission to access the Systems.

Levels of access will be granted as follows:

- i) **Edward employees** will be granted access based on their job functions and responsibilities; changes in access required by changes in responsibility shall be approved by the employee’s manager;
- ii) **Medical Staff members** will be granted access based upon their need for access in the care and treatment of their patients;
- iii) **Office Staff** will be granted access based upon the job functions and responsibilities of that staff member, and only for the Medical Staff member’s patients; any such Office member must have the Edward Medical Staff Office approval for computer access (Edward Medical Staff Office approval designee’s are maintained by the Application Security Team);
- iv) **Other non-employed individuals** will be granted access in accordance with the scope of duties and services to be performed under the terms of their contract. This access will be approved by the non-employee’s responsible Edward manager

Individuals must:

- i. maintain the confidentiality of their access credentials (e.g., user name, password, access code, etc.);
- ii. not allow another person to use one’s access credentials (e.g. user name, password, access code, etc.);
- iii. not use another person’s access credentials;
- iv. not access Protected Health Information (PHI) or any Edward confidential information for any purpose other than in accordance with their scope of duties and job functions;
- v. not access one’s own, one’s family members’, or any other known individual’s PHI for any purpose other than in accordance with their scope of duties and job functions;
- vi. not email passwords;
- vii. not e-mail PHI unless using encryption
- viii. not e-mail business confidential information unless using encryption;
- ix. only use portable devices with password protection and encryption enabled when working with PHI or business confidential information;
- x. report the following to the ISS Service Desk immediately:
  - a. Lost or stolen computing devices;
  - b. Suspicious, unsolicited e-mails. (Do not open them).
  - c. Unknown media (cds, flash drives, external hard drives, etc.) (Do not connect them to your computer or the network).
- xi. not give passwords over the phone. ISS personnel will never ask for password information over the phone or in e-mail correspondence;
- xii. not provide confidential information to anyone until you verify ID and the reason for their visit;
- xiii. log-off from an auto-login computer or lock your desktop computer when you leave it unattended to protect it from use by unauthorized persons
- xiv. not remove privacy screens attached to computer monitors
- xv. take care to protect confidential information from being viewed by onlookers;
- xvi. not hold secured doors open for unknown individuals without asking them to identify themselves;
- xvii. wear badge identification at all times while working.

**INFORMATION SYSTEMS CODE OF COMPLIANCE (p 2 of 2)**

Violations of Edward policies may result in the following:

- i. Edward employees will be subject to disciplinary action up to and including termination of employment;
- ii. Medical Staff members or members of their Office Staff may be deprived of access to the Information Systems; and
- iii. Independent contractors may be deprived of access to the Information Systems and their contract with Edward terminated.

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

**SOFTWARE POLICY:**

It is the policy of Edward to respect all computer software copyrights and to adhere to the terms of all software licenses.

- i. Individuals may not duplicate any licensed software or related documentation for use within the corporation or elsewhere;
- ii. Only software acquired through Purchasing and installed by Information Systems Services may be used on Edward computers;
- iii. Individuals are not permitted to bring software from home and load it onto Edward computers, or bring Edward system software home and load it onto home computers;
- iv. Duplication/installation in violation of the software policy will subject employees to disciplinary action up to and including termination of employment.
- v. Unauthorized duplication/installation by Medical Staff members or their Office Staff shall result in the termination of their access to the Edward Information Systems.

**ELECTRONIC SIGNATURE POLICY:**

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 password to any other person or permit another person to use it. I understand that patient information is confidential and agree to follow Edward’s policies and procedures. I understand that violation of Edward policies and/or the Information Systems Code of Compliance may result in action including, but not limited to, termination of remote electronic access and/or my employment.

**ACCEPTANCE:**

My acceptance of the Edward Hospital & Health Services Information Systems Code of Compliance constitutes my agreement that I will abide by all Edward policies and procedures applicable to Edward Information Systems (“Information Systems Policies”), including but not limited to Microcomputer Software and Hardware policy, the Information Systems Security policy and the Voice Mail and Electronic Mail Policy

I further agree to maintain the privacy and confidentiality of health care information in accordance with applicable State and Federal laws and TJC accreditation standards, including, but not limited to the new federal legislation found in 45 C.F.R. 164, et al., which implements the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

I recognize that Edward may monitor and/or audit my use of the Systems at any time. I agree to provide Edward with any documentation or information necessary for Edward to perform such monitoring/auditing, and to cooperate with Edward in performing such monitoring/auditing. I acknowledge that I have no expectations of privacy in regards to my use of the Systems.

Signature: \_\_\_\_\_

Name Printed: \_\_\_\_\_

Date: \_\_\_\_\_