 

**COMPUTER PASSWORD CONFIDENTIALITY POLICY**

**PURPOSE:**

It is the policy of Jamaica Hospital Medical Center, Flushing Hospital Medical Center & The

Jamaica Hospital Nursing Home to:

1. Ensure the confidentiality, integrity, and availability of electronic corporate and patient health information (ePHI). Confidentiality means that ePHI is not made available or disclosed to unauthorized people or processes. Integrity means that ePHI has not been altered or destroyed in an unauthorized manner, and availability means that ePHI is accessible and usable upon demand by authorized people.
2. Protect electronic corporate and patient health information from improper and unauthorized use while safeguarding its confidentiality, integrity, and privacy.
3. Monitor and/or identify users of electronic information by their assigned unique login.

The purpose of this Computer Password Confidentiality Policy is to establish a standard for creating, securing, and maintaining computer passwords. All computer network equipment must be protected by user authentication through the use of an individual’s unique user ID and a well-formed password. The scope of this policy includes all personnel who have access to the computer network, either on-site or remotely, of the above-mentioned entities.

**ACKNOWLEDGEMENT:**

I, the undersigned, acknowledge and agree that:

* I will be the only person to use my password and I will not disclose my password to anyone else, including family members, co-workers, management, technical support staff, administrative assistants, or secretaries.
* I will be held responsible for all activity performed with my user ID and password.
* I will apply the same guidelines to any remote, off-site access to the Hospital network.
* I will create a strong password, avoiding all words and phrases available in my public records, my habits or my personal details which can be used to guess my password (e.g., predictable words or phrases such as family member names, pet names, street names, birthdates, etc.).
* I will change my password every three (3) months in Compliance with IT Security Policy when prompted to do so by the system.
* I will not attempt to learn another user's password.
* I will not use the same password for Hospital accounts, as I do for other non-Hospital accounts (for example, personal email account, etc.). Where possible, I will not use the same password for various Hospital access needs.
* I will not write passwords down or store my password on-line. I will not insert passwords into email messages or other forms of unsecured electronic communication.
* I will not post it, or tape it on my machine or post it on materials inside a carrying bag.
* After I have signed into the hospital information system, I will not allow anyone else access to patient information except on a need-to-know basis. I understand that the improper and unauthorized use of patient information is considered a violation of security and can result in suspension or termination of employment.
* I understand that access to the hospital information system is for the purposes of rendering care to patients and at no time shall it be used for other purposes.
* If someone requests my password, I will deny their request and immediately notify the IT Department.
* If, at any time, I believe my password is compromised, I will immediately notify the IT Department and reset my password.
* I understand that confidential or proprietary information or identifiable patient data should never be transmitted (sent or received) over unsecured Internet Services, or through personal email, text messages or unsecured non-corporate mobile phones.
* I understand that upon termination of my employment, any authorization to use my password is immediately voided.
* If my position requires it, I will be using a computer password to electronically authenticate/sign patient data and/or reports recorded in the patient's permanent medical record. I will abide by all statements listed above with regard to computer password confidentiality.
* I understand that if I violate this policy, I may be subject to disciplinary action up to and including termination of my employment.

I have read and understand the Computer Password Confidentiality Policy and I agree to comply with all the terms stated.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

User's printed name: (Last, First, Middle Initial) Title: (eg, MD, RN, PhD, etc.)

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

User’s Employer’s Name Position Telephone ext.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date User's signature

Upon receipt of this document signed by the employee, the Information Technology department will issue a unique user login to the employee/department. The department will instruct the employee how to assign a personalized strong password to access the system.

A copy of this form goes to the following Departments:

• Human Resources Department

• Information Technology Department

• User's Department

Rev. 02/2022