HAMILTON MEDICAL CENTER
ORGANIZATIONAL POLICY

TITLE: Information Access **POLICY #** IM **PAGE** 1 **OF** 5

EFFECTIVE DATE: January 2020 **SUPERSEDES:** November 2017, November 2014, March 2013, December 2011**,** September 2011, January 2010, June2007, October 2006, January 2006, August 2005, January 2003

REFERENCE: TJC MANUAL

ATTACHMENTS: 1. Information Access Request
2. Computer and Information Usage Agreement
3. End User Agreement

AUTHORED BY: Director, Information Services

Purpose:

To establish a policy for assigning and maintaining security, HIPAA compliance, and access control to Hamilton Health Care's network and the clinical, financial and operational applications and data.

Policy:

The Information Access policy ensures the hospital complete control of systems access and maintains confidentiality of patient and associate data by allowing entry through the use of specific sign-on IDs and passwords. This policy also is meant to ensure that the user understands and attest to their understanding of HIPAA privacy and security rules as they relate to electronic protected health information and their usage of the HHCS network.

If possible, the sign-on ID should be a variation of user's initials and last name. Passwords are unique combination of at least ten characters, digits, and special characters used to gain access to the required system. Sign-on Ids will be assigned by the Security Administrator in the Information Services Department. Ancillary system managers will authorize sign-ons and passwords for their departmental systems, such as Pharmacy, Laboratory, and Radiology.

Department directors, supervisors, physicians and physician office managers may request sign-on IDs for those systems maintained by Information Services using the digital access request form at http://hhcs/Forms/UserAccess/index.asp, Information Access Request. This form refers to the Computer and Information Usage Agreement included in this policy. The user should review this agreement prior to signing Information Access Request from. Human Resources will collect the signature of the user on the End User Agreement form included in this policy and it will be kept in the employee file. The access request form is forwarded to Information Services once it is completed for sign-on assignment. The original form will be kept on file in the security manual and a copy will be

returned to the department director. Ancillary system managers should obtain an Information Access Request form prior to assigning the sign-on and the completed original should be stored in the ancillary department.

A three-business day turn around period will be required to set-up new sign-on ids. The user will be trained by their supervisor or departmental designee in the use of their sign-on/password and demonstrate proficiency when they are provided with the sign-on id. Sign-on Ids are for the exclusive use of the individual to which they are assigned. Where functionality is available, passwords will be setup to a default normal and will be set in a manor requiring that the user change them during initial sign-on. The user will not knowingly compromise their password by communicating it to any other person or post it on the computer.

Network passwords will expire every ninety (90) days and the users will be required to change their passwords. Where functionality is available, other system passwords will expire every ninety (90) days and the users will be required to change their passwords. Forgotten passwords will be reset by the Information Services Helpdesk. Proper identification will be required to change passwords or the department director or supervisor must authenticate the request. The help desk will reset the password or notify the Security administrator to do so. Where functionality is available, passwords will be reset to a default normal and will be set to expire immediately, requiring the user to change the password during initial sign-on.

If an individual believes that his or her password has been compromised, the password should be changed. If the system allows the user to revise their password, this should be done immediately.

Temporary access will be granted only to those needing access for a period greater than one week, and will follow that standard procedure for requesting access. Please contact Information Services management for any exceptions to this policy for access needed for less than one week. The user's department director or supervisor should notify information services in advance of any change in the user's job duties, responsibilities or employment status that may affect their need to access the system(s).

Human Resources forwards an employee termination and transfers listings to Information Services bi-weekly and sign-on IDs for these individuals are disabled or deleted from the systems. Sign-on IDs will also be disabled after 90 days of inactivity and deleted after 180 days of inactivity. Users also agree they will not disclose to any unauthorized person the application documentation or other vendor supplied information; remove or permit removal of such items from the hospital; or use any of these items for any purpose other than in the operation of the system.

Method of implementation:

1. An Information Access Request form should be completed and signed by a department director, supervisor, or physician to initiate the request. Physicians should receive the appropriate request forms from Medical Staff Services or contact Information Services. The

Educational Services director may also request access for new employees attending nursing orientation.

2. For those requesting Internet and Electronic Mail (E-mail) access, the policy IM.9, Internet and Electronic Mail (E-mail) Appropriate Use, must be reviewed.

3. Passwords will be assigned and maintained by the Information Services Security Administrator or the system coordinator for applicable ancillary systems. New access will be established within three business-days of receiving appropriate documentation.

4. The Security Administrator will notify the department director by phone, e-mail, or confidential interoffice mail concerning additions, changes, or deletions. An original request form will be maintained in Information Services. The department director will verify the additions, changes, or deletions and maintain a copy of the form in the associate's personnel file.

HAMILTON
HEALTH CARE SYSTEM

COMPUTER AND INFORMATION USAGE AGREEMENT

Hamilton Health Care System (HHCS) has a legal and ethical responsibility to safeguard the privacy of all patients and to protect the confidentiality of HHCS information. Security and confidentiality is a matter of concern for all persons who have access to HHCS information systems. Confidential information includes patient information, employee/volunteer/student information, financial information, or other information relating to HHCS. Confidential information is valuable and sensitive and is protected by laws like HIPAA and by strict HHCS policies. The intent of these laws and policies is to assure that confidential information will remain confidential. Users may learn of or have access to some or all of this confidential information through the HHCS information system. As an HHCS associate, physician, physician's office staff, student, or vendor with authorization to access data and resources through the HHCS information systems and network, you must read and comply with HHCS policies and practices.

Each person accessing data holds a position of trust relative to this information and must recognize the responsibilities entrusted in preserving the security and confidentiality of this information. All information about patients is strictly confidential. Patient information should not be discussed in public areas where others could overhear the conversation. Discussion of clinical information in public areas is not appropriate, even if a patient's name is not used. Confidential papers, reports, and computer printouts should be kept in a secure place. Confidential papers should be picked up as soon as possible from printers, faxes, copiers, and any publicly accessible location. If confidential papers do not become a part of the patient's medical file, they should be appropriately disposed of, i.e. shredded or placed in a confidential disposal bin, when they are no longer needed.

Users should only access information that is necessary for their job performance. Accessing any information other than what is required to do your job is a violation, even if you don't tell anyone else. Accessing data must not occur simply to satisfy a curiosity, such as a friend's birthday, address or phone number. Information should only be viewed when required for one's job. Access to HHCS systems or network requires a sign-on/username and password. Sharing this username/password instead of having your own is prohibited. Passwords should not be written down where others could find or use them. Users must not log on and let someone else use a computer under their password. Users should protect their data and computer against unauthorized use by logging off the computer system when leaving a workstation, turning off the computer or locking offices whenever possible.

The following specific principles of computer and network systems are applicable to all users:

- Respect the privacy and rules governing the use of any information accessible through the computer system or network and utilize information necessary for job performance job only.
- Respect the ownership of proprietary software. For example, do not make unauthorized copies of such software for your own use.
- Respect the finite capability of the system and limit your own use so as not to interfere unreasonably with the activity of other users.
- Respect the procedures established to manage the use of the system.
- Prevent unauthorized use of any information in files maintained, stored or processed by HHCS.
- Not seek personal benefit or permit others to benefit personally by any confidential information or unauthorized use of equipment.
- Not operate any non-licensed software on any computer provided by HHCS.
- Not exhibit or divulge the contents of any record or report except to fulfill by job duties.
- Not knowingly include in any record or report, a false, inaccurate, or misleading entry.
- Report any violation of these principles or HHCS policies or practices.
- Understand that all access to the systems may be monitored.
- Understand that obligations to these principles continue after termination of my employment. All users access are subject to periodic review, revision, and if appropriate access can be revoked.

Hamilton Health Care System End User Agreement

I have reviewed the computer and information usage agreement form and understand my obligations under this agreement. By signing this, I agree that I have read, understand and will comply with the agreement. If requesting Internet and Electronic Mail (E-mail), I also understand that Internet and e-mail access is a privilege and is to be used in an effective, ethical and lawful manner consistent with Hamilton's mission, vision and values. Further, I agree to adhere to the Internet and e-mail provisions and procedures contained in the **Internet and Electronic Mail (E-mail) Appropriate Use Policy**. I further attest to understanding my duties and role in protecting patient health information and will abide by the Organization's HIPAA policies. Failure to do so will result in a loss of system access, and may be subject to penalties, including disciplinary actions, under policies of Hamilton Health Care Systems and under laws of the State of Georgia to the extent applicable.

'Electronic signature' means a signature created, transmitted, received, or stored by electronic means and includes but is not limited to a secure electronic signature. The use of an electronic signature allows the authentication of a medical record by a healthcare practitioner. The healthcare practitioner may authenticate a record by entering a unique username and password into an electronic device and thereby create an individual "signature" on a record.

I have received training and understand the use of electronic signatures. The username and password I have accepted will be kept for my personal use only. I will protect the confidentiality of the password. If I feel the confidentiality of the password has been compromised, I will request another password. No other person will be allowed to use the username or password. Should the confidentiality of my password be compromised, I understand it is my responsibility to request a new password.

USERS SIGNATURE: _____ DATE: _____