HARRISHEALTH SYSTEM

POLICY AND REGULATIONS MANUAL

Policy No:	3.11.803
Page Number:	1 of 11
Effective Date:	04/ 2005
Board Motion No:	n/a
Last Revised Date:	09/11/2018
Due for Revision:	09/11/2021

TITLE **INFORMATION SYSTEM USER RESPONSIBILITY**

PURPOSE: To communicate to Harris Health System's computer system Users their responsibilities for ensuring a secure and well-managed computing environment.

POLICY STATEMENT:

Harris Health System (Harris Health) ensures the confidentiality, integrity, and availability of the computing environment by educating and training information system Users on their responsibilities for protecting electronic information. In accordance with applicable state and federal regulations, special attention is given to information systems that maintain or process Electronic Protected Health Information (ePHI).

POLICY ELABORATION:

This policy applies to all Harris Health Workforce members and Business Associates using or accessing Harris Health information or information systems

I. DEFINITIONS:

A. **CONFIDENTIAL INFORMATION:** Information that has been deemed or designated confidential by law (i.e., constitutional, statutory, regulatory, or by judicial decision).

B. **ELECTRONIC MEDIA:** Storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card.

C. **ELECTRONIC PROTECTED HEALTH INFORMATION (EPHI):** PHI that is created, received, maintained, or transmitted by electronic means.

D. **MALICIOUS SOFTWARE:** A program designed to damage or disrupts an information system (e.g., a virus).

E. **PROTECTED HEALTH INFORMATION (PHI):** Information that is created, received, transmitted, or maintained by Harris Health in any form or medium,

that relates to the patient's healthcare condition, provision of healthcare, or payment for the provision of healthcare, as further defined in the HIPAA regulations. PHI includes, but is not limited to, the following identifiers:

1. Name;
2. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:

    a. The geographic unit formed by combining all zip codes with the same three initial digits contains more than twenty thousand (20,000) people; and
    b. The initial three digits of a zip code for all such geographic units containing twenty thousand (20,000) or fewer people are changed to 000.

3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over eighty-nine (89) and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age ninety (90) or older;
4. Telephone numbers;
5. Fax numbers;
6. Electronic mail addresses;
7. Social security numbers;
8. Medical record numbers;
9. Health plan beneficiary numbers;
10. Account numbers;
11. Certificate/license numbers;
12. Vehicle identifiers and serial numbers, including license plate numbers;
13. Device identifiers and serial numbers;
14. Web Universal Resource Locators (URLs);
15. Internet Protocol (IP) address numbers;
16. Biometric identifiers, including finger and voice prints;
17. Full face photographic images and any comparable images; and
18. Any other unique identifying number, characteristic, or code, except as

permitted for re-identification purposes.

F. **RECORD:** Any item, collection or grouping of information that includes PHI and is maintained, collected, used or disseminated by or for the facility; the term "Record" includes (a) patient information originated by another healthcare provider and used by the facility to make decisions about the patient, and (b) tracings, photographs, videotapes, digital and other images that may be recorded to document care of the patient.

G. **SYSTEM ADMINISTRATOR:** The person who has responsibility for the operations of maintaining a computer system. Some operations include but are not limited to user account creation/modification/termination, system backups, and/or system configuration changes. These activities may be performed independent of, or in conjunction with, Harris Health Information Security and Information Technology.

H. **UNAPPROVED SOFTWARE:** Any application that has not undergone testing and approval by Harris Health Information Security.

I. **USER:** Any person who reads, enters, updates, sends, copies or prints information using any system regardless of the medium. Users must have an informational need to know, and must be authorized by the owner of the information.

J. **VIOLATION:** An infraction of a HIPAA policy, procedure, or safeguard that may or may not result in damage to Harris Health or exposure to liability.

K. **WORKFORCE:** Employees (permanent or temporary), volunteers, trainees, and other persons whose conduct, in the performance of work for Harris Health, is under the direct control of Harris Health, whether or not they are paid by Harris Health.

L. **WORKSTATION**: Any computing device that is used to store, view or manipulate Harris Health data whether connected to the Harris Health network or standalone. Examples include but are not limited to personal computers, laptops, mobile devices, or tablet personal computers.

II. ANTI-VIRUS PROTECTION:

A. Each Workstation accessing the Harris Health network has protection from malicious programs by up-to-date anti-virus software and anti-virus scans. Users shall not disable or attempt to disable the anti-virus software.

B. To protect against malicious programs being transmitted onto Workstations and into Harris Health electronic information systems, Users shall not download from the Internet any Unapproved Software, files, programs, and/or applications. Before a Workforce member downloads or uploads files, programs, or applications from/to the Internet, the User shall request approval by calling the Help Desk.

C. Users of Workstations shall not open any files attached to an e-mail from an unknown, suspicious or untrustworthy source and shall delete these attachments immediately because they may contain malicious programs.

III. LOGIN AND PASSWORD MANAGEMENT:

A. All applications/Workstations having access to ePHI or Confidential Harris Health information require a unique User ID and password. Users shall log into the application/Workstation using the User ID and password assigned to that User.

B. Users are responsible for keeping their User IDs and passwords confidential and are prohibited from sharing their User IDs and passwords with anyone. Users shall not write down their passwords or transmit them in e-mails or other forms of electronic communications including text messaging.

C. Users shall not log onto a Workstation using another person's User ID or badge nor shall the User permit another person to log on with his or her User ID or badge.

D. Users shall not enter data under another User's unique User ID and password.

E. Users shall lock or log off any time when leaving a Workstation unattended for

any reason. Users shall not allow others to use their Workstation session.

F. Users shall not attempt to mask their identity while logged into an application/ Workstation and/or Harris Health internal network.

G. Users shall not use passwords that are easily guessable, such as family names, pet Names, or birth dates.

H. If a User determines that another person has improperly obtained his/her User ID, password and/or badge or has improperly accessed Harris Health electronic systems through the use of the User ID, password, and/or badge the User shall contact Harris Health management and notify the Information Security Department immediately. System Administrators shall promptly disable access rights for that User ID.

I. For those information systems that lock User accounts after multiple failed login attempts, Users shall be aware that their account may be locked out due to an unsuccessful attempt by an unauthorized User trying to guess the User's password. If the User suspects that someone has attempted to guess his/her password, the User shall contact Harris Health Management and notify the Information Security Department immediately.

J. Users shall not let anyone else use their badge or reveal their password to anyone including Harris Health Information Security and Information Technology personnel.

K. Any exceptions to this section must be approved by the Chief Information Security Officer (CISO) or his designee.

L. Workforce members and Business Associates have no expectation of privacy in their work-related conduct or the use of Harris Health owned or Harris Health provided equipment or supplies. Workforce members and Business Associates should not expect privacy in the use or content of Workstations, media, or services.

IV. SECURITY INCIDENT REPORTING:

A. Users shall report instances of suspected security breaches involving ePHI, Confidential, or proprietary Harris Health information using the Harris Health Compliance Hotline at (800) 500-0333.

B. Security incident examples include but are not limited to:

1. Unknown/unauthorized individuals accessing information from a Workstation;
2. Unknown/unauthorized individuals viewing data on any computer screen;
3. Anyone requesting that a User provide them with the User's password;
4. A User attempting to login but the ID has been locked out after a number of failed login attempts;
5. Multiple Users logging into a system using the same User ID (except for a training class User ID);
6. Finding a User ID and password written down; or
7. Suspected Malicious Software on a Workstation.
8. User should report if their badge is lost or stolen.

V. TRANSPORTABLE MEDIA ACCOUNTABILITY DISPOSAL AND RE-USE:

A. Users shall not copy, store or remove from Harris Health facilities electronic Protected Health Information (ePHI) on any transportable device without written approval from the CISO and the Harris Health Privacy Officer and the data has been encrypted or protected with access controls approved by Information Security.

B. When information or data is stored on transportable or other media that is no longer needed, Users shall work with Information Security to physically destroy or securely erase the media that contains ePHI, Confidential, and/or otherwise proprietary information. Please refer to the Harris Health Records Retention Schedule (RRS) for the length of time a Record or document must be retained.

C. If electronic media is reused, procedures approved by the Information Security

Department will be used to ensure the information has been "wiped" and is no longer readable.

VI. E-MAIL/DATA SECURITY:

A. The use of encryption and/or digital signatures to protect the integrity of the data is optional for e-mail transmissions that remain within Harris Health network and e-mail system.

B. Whenever ePHI, Confidential, or otherwise proprietary information is being e-mailed or electronically transmitted to an external location or internet e-mail address, the use of encryption and/or digital signatures is required to protect the integrity and confidentiality of the information. Users who need to e-mail ePHI, Confidential, or otherwise proprietary information outside the organization should contact the Help Desk for instruction on how to encrypt those e-mails.

C. Other formats of ePHI, Confidential Harris Health information that require encryption when being electronically transmitted outside of the Harris Health network include but are not limited to:

1. FTP (File Transfer Protocol);
2. HTTP (Hyper Text Transfer Protocol); and
3. Instant Messaging.

D. Workforce members must comply with "3.11.310 Policy" when taking photographs in the workplace that contain patients or patient information in any form (i.e., patient's medical record, patient information on a computer screen, recordings etc.)

VII. DEVICE SECURITY:

A. The use of personal devices on the Harris Health network is not allowed. Any device used by a Harris Health Workforce member will be provided by the Information Technology Department and will contain the standard base configuration for Harris Health machines. Any exceptions to this will require written approval by the Information Security Department.

B. Users shall not install or connect hardware (e.g., USBs/hard disks/network cards) to any Workstation without prior approval from Information Security. Approval can be requested through the Help Desk.

C. Users shall not install or connect network devices (e.g., hubs/ /network cards/switches/wireless routers) or any other communication devices to the Harris Health network without prior approval from Information Security. Approval can be requested through the Help Desk.

D. Users will not attach or use any personal devices on any Harris Health PC or network device without prior approval from Information Security.

E. Users shall be responsible for protecting the information resources at Workstations for abiding by all information security policies. This includes but is not limited to:

1. Adjusting Workstation displays to ensure they cannot be seen from public walkways;
2. Placing privacy screens on displays that cannot be turned away from public view;
3. Logging out of all applications and locking the Workstation; or
4. Reporting incidents of Workstation or information system use that are prohibited by this policy.

VIII. LAPTOP AND TRANSPORTABLE MEDIA SECURITY:

A. Users shall review and adhere to security reminders that will be communicated on occasion through the e-mail system or other Harris Health publications.

B. Users shall be responsible for protecting the information resources contained on laptop and transportable computing devices and abiding by all information security policies. This includes but is not limited to:

1. When traveling, laptops and transportable devices are not to be checked as baggage;
2. Laptops and transportable devices are not to be left unattended or unsecured – especially at airport security checkpoints;

3. Laptops and transportable devices must require a User ID and password prior to allowing access to ePHI;
4. Encryption of data or information to provide additional access control as warranted;
5. Users are required to bring in their laptop every 30days to ensure that the anti-virus is updated as well as other software;

C. If a transportable device containing ePHI is lost or stolen, the incident must be reported to the Information Security Department, and when appropriate to the Police Department and/or facility management within twenty-four (24) hours. Lost devices containing Harris Health ePHI, Confidential or otherwise proprietary data are subject to remote wiping for the protection of Harris Health information.

D. Asset tags attached to laptops and/or transportable devices are not to be removed for any reason.

IX. REMOTE ACCESS SECURITY:

A. Harris Health shall allow Users to connect remotely to the information systems in accordance with the procedures below:

1. Users who have been granted remote access privileges shall not permit third parties to access Harris Health information systems via such remote access.
2. Users shall be responsible for giving their remote access connection the same consideration and protection as Users give their onsite connection.
3. Users shall be held accountable for any unauthorized use or for any breaches of security resulting from User's remote access capability and may be subject to discipline under Harris Health Policy 3.11.104 "Sanctions for Failure to Comply with Privacy and Information Security Policies."

B. Users will be required to use dual factor authentication which will require user id, password and a token remote access to the Harris Health network using any type of remote connectivity must not configure the connection icon to automatically remember the User's remote account password. Remote connections include

but are not limited to Citrix and/or Virtual Private Network (VPN).

C. Harris Health Information Technology requires that remote Harris Health computers be installed with the most recent security updates for the operating system. The computer must also have anti-virus software installed, functioning, and updated with the latest virus definition file provided by the vendor. If security updates have not been applied, Harris Health will use electronic means to install updates and anti-virus software for computers attempting a remote connection to the Harris Health network.

X. SANCTIONS:

Violations of this policy are subject to the Harris Health policy 3.11.104 "Sanctions for Failure to Comply with HIPAA Privacy and Security Policies."

REFERENCES/BIBLIOGRAPHY:

Harris Health System Policy and Procedures 3.11.104 Sanctions for Failure to Comply with HIPAA Privacy and Security Policies

Harris Health System Policy and Procedures 3.11.800 Information Security

Harris Health System Policy and Procedures 3.11.808 Information Security Awareness and Training

Harris Health System Policy and Procedures 3.11.809 Information Security Password

OFFICE OF PRIMARY RESPONSIBILITY:

Harris Health System Office of Corporate Compliance

REVIEW/REVISION HISTORY:

Record reviews and revisions below:

Effective Date	Version # (If Applicable)	Review or Revision Date (Indicate Reviewed or Revised)	Reviewed or Approved by: (If Board of Managers Approved, include Board Motion #)
04/20/2005	1.0	New	President/CEO
		Reviewed 06/20/2006	Information Security Official
		Reviewed 07/28/2008	Information Security Official
07/28/2008	2.0	Revised 07/28/2008	President/CEO
06/01/2009	2.1	Revised 5/01/2009	President/CEO
		Revised/Approved 05/13/2014	Operations Policy Committee
		Approved 09/11/2018	Interdisciplinary Clinical Committee