TITLE: **INFORMATION ASSET SECURITY/USE**

PURPOSE: To establish responsibilities and requirements for the protection and proper use of University Health information assets as they relate to data, image, text and voice accessed through internal and external systems by employees, contractors, and other users. To prevent misuse and loss of information assets; establish the basis for audits and self-assessments; and preserve management options and legal remedies in the event of asset loss or misuse. This is a revised policy and supersedes policy dated 06/26/13. [Key Words: Information Assets, Information System Access, Security, Protected Health Information, Electronic Medical Record (EMR)]

POLICY STATEMENT:

University Health will protect the integrity and confidentiality of all information assets, while providing access to authorized users. University Health reserves the right to monitor any and all aspects of user activity to ensure compliance with this policy.

SCOPE STATEMENT:

This policy is applicable to all information assets and services which support University Health business and clinical activities, and covers all staff, consultants, contractors, and other persons or third parties accessing or using the University Health's information assets. There may be additional policy and/or departmental requirements for use of these resources, services, and authorization for access to, and release of, information. Fulfillment of information asset security responsibilities is mandatory and may be considered a condition of continued access or employment.

NOTE: Biomedical devices are excluded in this policy.

University Health must ensure that information is available, updated, and properly maintained so that quality continuity of care is provided across inpatient and outpatient environments. All individuals participating in the care of University Health patients are required to use information systems and other such information assets provided and maintained by University Health.

POLICY ELABORATION:

I. DEFINITIONS

A. **Biometric Scan** – any process used to validate the identity of a user who wishes to sign into a system by measuring some characteristic of that user. Biometric samples include finger prints, retinal scans, vein scans, face recognition, and voice scans.

B. **Department Head** – a University Health department director or above and credentialed individuals through partnered entities.

C. **Encryption –** the process of transforming electronic information using a key mechanism to make it unreadable to anyone except authorized users.

D. **General Controls** - IT General Controls are controls that apply to the entire IT infrastructure. These controls include policies, procedures and practices that specific objectives will be achieved; which are to ensure the proper development and implementation of applications and the integrity of program and data files and of computer operations. These controls can include access controls, system development life cycle controls, change management controls, IT physical security controls, system and data backup and recovery controls and computer operation controls.

E. **Information Assets –** include, but are not limited to, data, text, image, voice, computers, file servers, storage array, storage switches, workstations, laptops, software, printers, modems, printed reports, voice and data mobile wireless devices, portable storage media, such as flash drives, and internal or external communications networks (Internet, commercial online services, and electronic mail systems) that are accessed directly or indirectly both into and from the University Health's computer facilities, excluding Biomedical devices.

F. **Information Security** - a set of strategies for managing the processes, tools and policies necessary to safeguard data from unauthorized access or modification, whether in storage, processing or transit, to ensure its availability, confidentiality and integrity. Sensitive information is only disclosed to authorized individuals (confidentiality), unauthorized modification of information is prevented (integrity) and data can be accessed by authorized users when needed (availability).

Information Security includes physical security and logical security. Physical security is the protection of information assets from physical events such a fire, flood, natural disasters, theft, vandalism and terrorism. Logical security are the techniques that protect computers, networks and data from unauthorized access or attacks and is comprised of application security, network security and disaster recovery.

G. **Information Services –** a University Health division, comprising the Office of the CIO and all reporting departments.

H. **Jailbroken or Rooted Devices** – the act of unlocking a phone to give it capabilities beyond those permitted by the manufacturer that made it and giving someone full control of the device. Jailbroken applies to iOS devices and Rooted refers to Android.

I. **Negligence –** the failure to use such care as a reasonably prudent and careful person would do under similar circumstances.

J. **Non-interactive Task –** a job scheduled to run automatically or one that is triggered by a series of events and does not depend on user input and can be scheduled to occur on multiple systems at any time.

K. **Protect –** includes preventing misuse, abuse, loss, theft, or unauthorized access or disclosure of information assets.

L. **Protected Health Information (PHI) –** any information, whether oral, written, electronic, or recorded in any form or medium (including demographic information that is collected from an individual), that identifies or may be used to identify the individual and relates to:

1. past, present or future physical or mental condition of an individual
2. providing health care to an individual
3. past, present or future payment for the provision of health care to an individual.

For additional information see 2.14 Attachment I: HIPAA Privacy Guidelines: Uses and Disclosures of Protected Health Information

M. SPAM email – an unsolicited message sent in bulk.

N. **User –** all employees, contractors, and other persons or third parties authorized to access or use University Health computers, telecommunications equipment, or other information assets.

O. Vendor - an entity (including Vendor Personnel as defined below) that performs services under an agreement; and/or is granted access to University Health networks, computing environments and/or confidential information.

P. Vendor Personnel - all Vendor employees, contractors, sub-contractors, suppliers and agents provided access to University Health networks, computing environments and/or confidential information.

II. RESPONSIBILITIES

The hardware and software systems belong to University Health and must be used for business/management-approved purposes only. Any product developed or created while using these systems is the property of University Health. University Health reserves the right to monitor any and all aspects of user activity to ensure compliance with this policy.

A. Department Head

Department heads are responsible for the following:

1. Maintaining a current list of the assets and services for which they are accountable, as well as the applicable control requirements

2. Authorizing users' access to information assets and ensuring that these assets are used for management-approved purposes only

3. Responding in a timely, effective manner to loss or misuse of information assets and to identified information asset security exposures

4. Authorizing access-level changes (including access origination, transfers and termination) and assigning custody

5. Notifying the appropriate Information Services departments of new hires, transfers, terminations and status changes of user accounts

6. Periodically reviewing and updating the list of authorized individuals with access to restricted information assets

7. Ensuring the data they receive, create and release are secure

8. Ensuring that Information Services security administration controls and oversight of information assets are in place

9. Ensuring subordinates are trained and aware of downtime procedures

B. User

Users are responsible for the following:

1. Complying with information asset security and application system controls

2. Using information assets only when authorized by management and only for approved purposes

3. Ensuring that passwords meet specified requirements, are not shared, and are properly protected

4. Reporting security exposures, misuse or non-compliance situations to management attention

5. Ensuring confidentiality of information accessed and accessing only information pertaining to their job functions, including upon termination of access.

6. Ensuring that computers or equipment that connect to University Health computers or networks, which are not on University Health premises and not under University Health control must be used for approved management purposes; must maintain appropriate measures; and must have confidentiality agreements and/or other appropriate contracts in effect

7. Users must allow any portable storage devices they connect to University Health-owned PCs, laptops, and tablets to be encrypted before any information can be transferred

8. Insuring they are trained, and are familiar with downtime procedures and location of downtime documents

C. Information Services Staff

Designated Information Services staff members are responsible for the following:

1. Administering information asset security and application system controls in their custody

2. Providing security controls for protection of information assets

3. Effectively communicating access control rules and restrictions to users

4. Providing safeguards to prevent unauthorized attempts to gain access to data or restricted areas

5. Obtaining authorization for work station location and use

6. Establishing security administration controls and oversight of all University Health software applications to maintain standardized security administration

D. Vendors and Vendor Personnel

Vendors are responsible for the following:

1. Annual completion of a security risk assessment

2. Implementing a comprehensive information security program based on an appropriate Security Framework

3. A security awareness training program for all vendor personnel that will access University Health systems and data

4. Complying to the Health System Cybersecurity Standard Terms and conditions Amendment where applicable

5. Prompt notification when vendor personnel no longer require

access to University Health systems and data

III. SECURITY REQUIREMENTS

A. Access will be assigned according to the user’s job function and the user must sign a confidentiality agreement.

B. Users may not attempt to access or gain access to data for which they do not have direct responsibility or authorization to access.

C. User IDs follow Information Services standards to maintain consistency across computing platforms.

1. Generic user IDs and passwords are not permitted for employee use as an entry point for any application program.

2. Generic access to information is allowed only for non-interactive tasks. Generic account passwords must be protected from unauthorized disclosure.

3. Training accounts are allowed for training use only, and all use must be documented for accountability.

4. Hard-coded passwords that reside on a client machine or in an application must be afforded reasonable protection commensurate with risk and the available platform or application security features.

5. Passwords are set to automatically expire at system-defined intervals.

D. Users are responsible for any action taken under their user IDs and passwords. All user-chosen passwords must be complex. Passwords are to be kept confidential and not shared.

E. All users will complete the required e-learning course to include security awareness and phishing awareness training. Users must pass required courses before granted access to Epic or email accounts.

F. Fraudulent, harassing, embarrassing, indecent, profane, threatening, obscene, intimidating, sexually explicit, or other unlawful material may not be sent, accessed, displayed or stored on the University Health's information assets. Users encountering or receiving such material should immediately report the incident to their supervisors and/or the Integrity Office.

G. Use of the Internet must be in compliance with all University Health policies, and may not be used for personal financial gain in accordance with University Health's conflict of interest policy.

H. Internet addresses that are deemed inappropriate or not conducive to the work environment are blocked. Internet activity is monitored and recorded. Internet filtering software does not substitute for individual judgment.

I. Sites blocked with a "continue" option may be accessed only when access is required for business purposes. Users may request blocked sites that have legitimate research or business value be allowed.

J. All information stored on external media, must be encrypted.

K. Software purchased by University Health is to be used for approved purposes only. All purchased software is company property and is subject to the license agreement as specified by the vendor and/or modified by University Health contract. Any duplication or alteration of licensed software, except for backup purposes, is strictly prohibited.

L. Users are not permitted to load or download any software onto their workstation or the network, this includes any software prompted requests for version updates or patches. Such requests for software must be approved and installed by Information Services to ensure the software can be certified to work in the University Health's computing environment, and to protect from computer viruses, tampering and other exposures.

M. In the event unauthorized and/or unapproved software is discovered on an individual computer or on the network, the computer may be formatted and reconfigured immediately without notice.

N. Computers owned by and located within University Health facilities are programmed to automatically lock the workstation when the computer receives no input for a specified period of time.

O. To eliminate or minimize the possibility of unauthorized access to PHI and other confidential information, all University Health workstations will be located in a manner that reduces the likelihood of information being viewed by unauthorized individuals.

P. When users leave their workstations they must either lock the workstation, disconnect, or log off the system. Users should log off at the end of their shifts.

Q. Computer servers and supporting infrastructure must be administered as areas of restricted access when continued operation is considered essential or where confidential and sensitive information is stored.

R. Information Services maintains a plan for responding to information system emergencies that includes performing backups, preparing critical facilities to provide continuity of operations and recovery. Alternate modes of operation that may include manual methods must be documented by each department to ensure continuity of critical services.

S. Hardware acquired, installed, added, removed, connected/disconnected, or moved from University Health infrastructure network or facilities must be authorized and performed only by Information Services.

T. PHI may not be transmitted over any communication device unless secured through Information Services.

U. Hardware and software applications are considered University Health assets and fall under University Health Policy No. 6.04, Asset Management.

V. Any loss of information assets due to negligence will require the user to reimburse University Health for the replacement cost of the item.

W. A user cannot attempt to limit or restrict the University Health's right to monitor any and all aspects of the computer system.

X. Software vendors who require access for diagnostic/support purposes will be required to gain access via a secured account that remains in the disabled state until needed. User accounts must not allow more system or network privileges than necessary to meet contract requirements.

Y. Personal computing devices (e.g., laptops, tablets, PDAs and voice and data wireless devices) are not permitted to connect to University Health network unless authorized by Information Services.

Z. To protect the integrity of data, tasks involved in critical business processes must be performed by separate individuals. Where feasible, responsibilities of programmers, system administrators, and database administrators must not overlap.

AA. All systems connected to the network will have active virus protection where technologically feasible.

BB. All critical information used on workstations will be placed on networked file server drives to allow for backup. PHI, confidential, or proprietary information may not be stored on the

Local Disk (C:), or Desktop, even temporarily.

CC. Proof of identity for password resets is required and may include personal information held in central database records, last 4 digits of the Social Security Number, photo ID or human factor such as a biometric scan, and satisfactory challenge-responses in a self-service application. Accounts will be restricted from login if the user cannot be identified with one of these methods.

DD. User network accounts that have not been accessed for a period of 100 days will be deleted and the user will be required to reapply to re-establish access.

EE. All hard drives on University Health-owned PCs, laptops, and tablets must be equipped with disk encryption. Only encryption products approved by Information Services and configured according to standards set by Information Services may be used. Encryption of Encryption of existing hard drives is required unless documented approval from Information Services has been obtained. Attempting to bypass, penetrate, alter the configuration of, or otherwise affect the operation of any encrypted hard drive(s) is a violation of this policy.

FF. Information Services is responsible for application software University Health runs and ensures IT general controls are enforced. Authorization must be obtained from the Sr. Vice President/CIO before proceeding with any acquisition, development, implementation, operation, or maintenance of information assets.

GG. Any mobile device used to access or store University Health data must use approved mobile device software. Jailbroken or rooted devices will not be permitted to access University Health data or network, and the device operating system must be on a current, supported level. The mobile device software will require a passcode and automatically lock the data after a predetermined time. Any data contained within the mobile device software will be wiped from the device when a user has a change in status resulting in a loss of entitlement to the data.

HH. All remote access to University Health systems and data must be authorized and may be used for approved business purposes only. Additional remote access to specific end points requires additional approval from the Sr. Vice President/CIO prior to issuance.

IV. EMAIL REQUIREMENTS

A. Policy Guidelines/Perspective

a. The email system should be reserved for conducting business related to University Health. It may not be used to create, forward, or attach any offensive or disruptive content.

b. All messages drafted, sent or received on the email system are, and remain, the property of University Health. These messages are not the private property of any employee, contractor, or user of the system.

c. University Health reserves and will exercise the right to review, audit, intercept, block, access, and disclose all messages received or sent over the email system for any purpose. The contents of any email may be disclosed without the permission of the user.

d. University Health employs software to automatically block spam email.

e. Due to the changing trends in virus contamination, allowable file type attachments will be permitted at the discretion of Information Services.

B. Staff Responsibilities

a. The email system may not be used to send or receive copyrighted materials or confidential/proprietary information without authorization.

b. All email sent externally (to email addresses outside University Health) containing PHI must be encrypted by the sender by typing “PHI:” anywhere in the subject line.

c. Email messages should be treated as confidential and accessed only by the intended recipient. The user is responsible for ensuring the accuracy of the email address of the intended recipient. All inbound and outbound emails will contain a system-generated disclaimer.

d. Email signatures are digital business cards, providing contact information for University Health staff members and representing the University Health brand. Employees are not required to create an email signature however, those who choose to do so must follow a standard template outline, as required for print business cards. See Attachment I.

e. Email that is sent internally to University Health must be directed to the appropriate audience. Discretion must be used in identifying those who are copied or blind copied. The email system may be used for corporate-wide (all users) communications, if approved by area vice president, Corporate Communications and the Executive Vice President/CIO of Information Services or designee.

C. Reporting

a. Suspicious emails must be reported to Information Services. A reporting mechanism will be provided and any emails determined to be phishing will be blocked.

V. EMAIL RETENTION REQUIREMENTS

Users are accountable for knowing what constitutes a record that must be kept for a specified period of time, according to the Texas State Library and Archives Commission Local Schedules GR, HR, and PS, or industry-specific standards such as The Joint Commission, CMS, HIPAA, and state regulatory boards.

A. Email correspondence will be kept for a maximum of four years and will be removed on a rolling basis.

B. Exceptions to the four-year retention period may be requested by application to the University Health President/CEO for individuals whose email correspondence falls under longer, regulatory or legal retention requirements.

C. "Trash" in the Outlook Deleted Items Folder is retained for 90 days and deleted from user mailboxes on a rolling nightly basis.

D. Email is subject to legal discovery. All government records, regardless of the medium in which each is maintained must be retained in condition. They may not be destroyed if any litigation, claim, negotiation, audit, public information request, administrative review or other action involving the record is initiated prior to its destruction. The record remains in its condition until completion of the action and the resolution of all issues that arise from it, or until the expiration of the applicable retention period, whichever is later.

VI. TELEPHONE SYSTEM REQUIREMENTS

A. Security software is installed on all University Health phone switches. This software is used to monitor, secure and track call activity. Users on recorded lines must state required disclaimers when answering a call.

B. Area codes or prefixes that are deemed inappropriate, or have the possibility of per-minute charging will be blocked.

C. Long distance calls require the use of an access code to complete the call.

D. The use of cell phones is permitted within University Health. Discretion must be used, however, to ensure patient care is not disrupted or compromised. Photography is prohibited on and in University Health property and leased facilities without proper authorization, per UH Policy No. 9.02, Patient's Right to Consent.

E. Patient and confidential information may be left on voice mail only if verification that voice mail and not an answering machine is being used. Otherwise, a call-back number is to be left where the caller can be reached. Patient and confidential information must not be left on answering machines.

F. To prevent unnecessary costs to University Health, users should not use 1-411 for information.

G. University Health will not incur additional costs for personal phone usage to include phones, cell phones, and long distance use. Each user is responsible for any of these additional charges.

VII. POLICY VIOLATIONS

Users encountering violations of this policy must report the incident(s) immediately to their supervisors and/or the Integrity Office. Information Services should be notified immediately of incidents where assets are at risk. The supervisor is responsible for notifying the Integrity Office if the violation was not reported. Each incident will be reviewed on an individual basis, and where appropriate, the supervisor may need to take disciplinary action, up to and including termination of employment or a contract. In addition, Information Services may revoke access to computer systems assets, if the violation is determined to put such resources at risk. University Health reserves the right to pursue legal action as needed. Violations of state and federal law may subject persons to penalties of fines or imprisonment or both.

REFERENCES/BIBLIOGRAPHY:

University Health Policy No. 2.12, Conflicts of Interest

University Health Policy No. 2.13, Reporting Errors and Incidents of Misconduct

University Health Policy No. 2.14, HIPAA Compliance Program

Policy No. 7.04, Asset Management

University Health Policy No. 9.02, Patient's Right to Consent To Treatment

University Health Policy No. 10.03, Medical Records

University Health Information Services Standards Manual

Public Law 104-191, "Health Insurance Portability and Accountability Act of 1996"

IT Governance BS7799/ISO 17799

National Institute of Standards and Technology Special Publications 800 series

Texas State Library and Archives Commission Local Schedules GR and HR, effective April 17, 2016

OFFICE OF PRIMARY RESPONSIBILITY:

Vice President/Chief Information Officer

ENDNOTE:

"If records are stored electronically, they must remain available and accessible until the retention period … along with any hardware or software required to access or read them. Electronic records may include electronic mail (e-mail), websites, electronic publications, or any other machine-readable format. Paper or microfilm copies may be retained in lieu of electronic records." – *Texas State Library and Archives Commission Local Schedule GR, April 17, 2016*