TITLE: **INFORMATION ASSET SECURITY/USE**

PURPOSE: To establish responsibilities and requirements for the protection and proper use of University Health System (Health System) 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 05/27/10. [Key Words: Information Assets, Information System Access, Security, Protected Health Information, Electronic Medical Record (EMR)]

POLICY STATEMENT:

The Health System will protect the integrity and confidentiality of all information assets, while providing access to authorized users. The Health System 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 Health System business and clinical activities, and covers all staff, consultants, contractors, and other persons or third parties accessing or using the Health System'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.

The Health System 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 Health System patients are required to use information systems and other such information assets provided and maintained by the Health System.

POLICY ELABORATION:

I. DEFINITIONS

A. 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 Health System's computer facilities.

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

C. Department Head – a Health System department director or above, who identifies, classifies, creates, maintains, and secures information assets within his or her areas of responsibility.

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

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

F. SPAM e-mail – an unsolicited message normally sent in bulk.

G. Information Services – a Health System division, comprising the Office of the CIO, Business Information Systems, Clinical

Systems, Infrastructure Services, Data Center Operations, Computer Training, Data Security Administration, Biomedical Engineering, IT Service Delivery, Corporate Records Library, Project Management, Disaster Recovery, and HIPAA Security Compliance Management.

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

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

J. Non-interactive Task – a job scheduled to run automatically or one that is triggered by a series of events

K. 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.

II. RESPONSIBILITIES

The equipment and access given to employees are to assist them in performing their jobs. The hardware and software systems belong to the Health System and may be used for business/management-approved

purposes only. Any item developed or created while using these systems is the property of the Health System.

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), assigning custody, and authorizing release of information

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

B. User

Users are responsible for the following:

1. Complying with information asset security and application system controls

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

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

4. Complying with access control requirements

5. Bringing security exposures, misuse or non-compliance situations to management attention

6. Maintaining confidentiality of information accessed and accessing only information pertaining to their job functions

7. Ensuring the security of confidential information continues upon termination of access.

C. Information Services Staff

Designated Information Technology Services staff members are responsible for the following:

1. Administering owner-specified information asset security and application system controls for information and information processing assets in their custody

2. Providing and administering access to information assets

3. Providing and administering physical and procedural safeguards for protection of information assets

4. Effectively communicating access control rules, and restriction to users

5. Providing for timely detection of, and effective response

to, unauthorized attempts to gain access to data or restricted areas

6. Ensuring work station location and use are authorized

7. Bringing security exposures, misuse, or non-compliance situations to management attention

8. Establishing centralized security administration controls and oversight of all Health System software applications to maintain centralized security administration

III. GENERAL REQUIREMENTS

A. Access to Health System information assets is restricted to authorized individuals and used only for business/management approved purposes. All requests for access must be approved by the department supervisor and the appropriate Information Services Department. 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 all computing platforms.

1. Generic user IDs and passwords are not permitted 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. 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.

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

5. Users are responsible for their user IDs and passwords. All user-chosen passwords must be difficult to guess. Users must never write down or otherwise record a readable password and store it near the access device to which it pertains. Passwords are to be kept confidential and not shared. Any action taken under that user ID and password will be the sole responsibility of the owner of that user ID and password.

D. All users will complete the required e-learning course before being granted access to Health System computer systems. This will include security awareness training.

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

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

G. 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. Allowed sites that are deemed inappropriate may not be accessed. Users are responsible for

reporting sites with objectionable content that is not blocked. 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.

H. Sensitive programs, restricted utilities, and other elements that may be used to bypass established controls must have procedures to prevent unauthorized use, reproduction or modification. Historical data and/or logs of usage of such elements/programs facilities must be available on demand.

I. Internal applications under development, or undergoing major modification, whether the work is done within Information Services or elsewhere, should be reviewed and approved by the application owner and Information Services Change Advisory Board for information asset security compliance before becoming operational in a production environment. Change management ensures that changes do not introduce any new vulnerability to systems or processes, and that changes do not remove important existing features.

J. PHI/sensitive information stored on portable or fixed storage media, (e.g., CD, DVD, thumb drive), must be deleted or destroyed when no longer required. All stored media must be destroyed prior to disposal. The media may be forwarded to the director of Environmental Services for destruction.

K. All access to external systems must be approved by Information Services. Consideration must be given to the security of the electronic transmission of information. Security measures, such as Encryption, may be appropriate.

L. Computers or equipment that connect to Health System computers or networks, which are not on Health System premises and not under Health System control, when used to access Health

System information, must be used for approved management purposes; must maintain appropriate measures; and must have confidentiality agreements and/or other appropriate contracts in effect. The Information Asset/Security Use Policy remains in effect when accessing the system remotely.

M. Software purchased by the Health System 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 the Health System contract. Any duplication or alteration of licensed software, except for backup purposes, is strictly prohibited. Individuals 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 Health System's computing environment, and to protect from computer viruses, tampering and other exposures.

N. 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.

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

P. To eliminate or minimize the possibility of unauthorized access to PHI and other confidential information, all Health System workstations will be located in a manner that reduces the likelihood of information being viewed by unauthorized individuals. In the event the workstation cannot be located in this manner, a privacy screen will be installed on the monitor.

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

R. Computer servers and supporting facilities, as determined by management, must be administered as areas of restricted access when continued operation is considered essential or where confidential and sensitive information is stored.

S. Information Services will establish/maintain a plan for responding to a system emergency that includes performing backups, preparing critical facilities to provide continuity of operations in the event of an emergency, and recovering from a disaster. Alternate modes of operation that may include manual methods must be documented by each department to ensure continuity of critical services in the event of a system emergency.

T. Hardware acquired, installed, added, removed, connected/disconnected, or moved from Health System infrastructure network or facilities may be authorized and performed only by Information Services. Information Services will maintain an electronic inventory of all computing devices and network hardware.

U. PHI may not be transmitted over any communication device unless authorized by Information Services.

V. No hardware or software applications may be removed from Health System's premises without written authorization from Information Services. Logs will be maintained of all equipment removals.

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

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

Y. Users must not leave printers unattended while printing PHI and other confidential information. An exception will be made if the area surrounding the printer is restricted such that persons who are not authorized to see the material being printed may not access it.

Z. 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.

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

BB. 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.

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

DD. 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.

EE. Students or former students who have student accounts and who are subsequently hired as employees will normally be given an additional staff/faculty account.

FF. 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.

GG. 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.

HH. All hard drives in Health System-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 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.

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

JJ. Information Services is responsible for all information systems initiatives. All information systems activities will be reviewed by the Vice President/CIO. Authorization must be obtained from the Vice President/CIO before proceeding with any acquisition, development, implementation, operation, or maintenance of information assets.

KK. Computer monitors, keyboards, and mice in patient care areas must be cleaned daily with Infection Control-approved disinfectants. All computer equipment (except computer

monitors) and computer cables in patient areas must be disinfected upon discharge or transfer of a patient.

IV. E-MAIL REQUIREMENTS

A. The e-mail system may not be used to create, forward, or attach any offensive, disruptive messages or chain letters.

B. The e-mail system may not be used to send (upload) or receive (download) copyrighted materials, trade secrets, proprietary financial information, or similar materials without authorization from the user's immediate supervisor.

C. All messages composed, sent or received on the e-mail system are and remain the property of the Health System. These messages are not the private property of any employee, contractor, or user of the system.

D. Notwithstanding the Health System's right to retrieve and read any e-mail messages, such messages should be treated as confidential by other employees and accessed only by the intended recipient. It is the user's responsibility to ensure the accuracy of the e-mail address of the intended recipient. All inbound and outbound e-mails will contain a system-generated disclaimer.

E. E-mail that is sent internal to the Health System must be directed to the appropriate audience, and apply to all recipients. Discretion must be used in identifying those who receive carbon or blind copies. The e-mail system may be used for corporate-wide (all users) communications, if approved by the area vice president or designee, Corporate Communications, and the Vice President/CIO of Information Services or designee.

F. All e-mail sent via the Internet containing PHI must be encrypted. To encrypt an e-mail, type "PHI:" anywhere in the subject line.

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

H. The Health System will employ software to automatically block any Spam e-mail.

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

V. E-MAIL 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.

Generally, the retention procedure is as follows:

A. E-mail correspondence will be kept in the user's network account for a maximum of three years and will be removed from user mailboxes, folders, and archives on a rolling basis determined by the technological requirements of the Health System's contracted exchange application.

B. Exceptions to the three-year retention period may be requested by application to the Health System President/CEO for individuals whose e-mail correspondence falls under longer, regulatory or legal retention requirements. Failure to retain records for the appropriate period of time is a violation of the law.

C. "Trash" in the Deleted Items Folder is retained for 90 days and

deleted from user mailboxes on a rolling nightly basis.

D. E-mail is subject to discovery. No local government record, regardless of the medium in which it is retained, may be destroyed if any litigation, claim, negotiation, audit, public information request, administrative review or other action involving the record is initiated prior to the destruction of the record until the 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. FACSIMILE REQUIREMENTS

A. Transmission of PHI via facsimile (fax) is restricted to information required for continuity of care where other means of delivery are not appropriate.

B. All facsimiles must be accompanied by Health System-approved cover sheets provided on the Health System Intranet Homepage. Individual or departmental cover sheets are not permitted under any circumstances. Faxes containing PHI must use the Confidential Health Information cover sheet.

C. If PHI is to be sent by fax, the recipient must first have been notified of the time when it will be transmitted, and also have agreed that an authorized person will be present at the destination machine when the material is sent. An exception will be made if the area surrounding the fax machine is restricted such that persons who are not authorized to see the material being faxed may not enter.

D. The sender of an outgoing fax is responsible for ensuring that the outgoing fax was sent to the correct destination by confirmation receipt. Written notification must be provided and filed with the Chief Privacy Officer for any misdirected faxes of PHI.

E. PHI, whether inbound or outbound, is not to remain in or around fax machines.

F. Fax machines that send PHI should be pre-programmed to destination numbers whenever possible to eliminate errors in transmission from misdialing. These numbers should be verified for accuracy on a monthly basis.

VII. TELEPHONE SYSTEM REQUIREMENTS

A. Security software is installed on all Health System 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. All charges related to the call are billed to the appropriate responsibility center.

D. The use of cell phones is permitted within the Health System. Discretion must be used, however, to ensure patient care is not disrupted or compromised. The use of camera phones for the purpose of taking pictures is prohibited on and in Health System property and leased facilities without proper authorization, per the Patient's Right to Consent policy.

E. Users are prohibited from connecting modems of any type to the Health System communications infrastructure. Requests for modems must be approved and installed by Information Services.

F. Users are prohibited from connecting phones of any type to the Health System communications infrastructure. Requests for phones must be approved and installed by Information Services.

G. 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.

H. To prevent unnecessary costs to the Health System, users should not use 1-411 for information. A phone directory is available online that contains the Yellow, White, and Business pages for San Antonio and surrounding areas.

I. The Health System 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.

VIII. 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 in 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. The Health System 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:

Health System Policy No. 2.12, Conflicts of Interest

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

Health System Policy No. 2.14, HIPAA Compliance Program

Health System Policy No. 9.02, Patient's Right to Consent

Health System Policy No. 10.03, Medical Records

Health System Information Services Standards Manual, 2010

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 3, 2011

OFFICE OF PRIMARY RESPONSIBILITY:

Vice President/Chief Information Officer

ENDNOTE:

"Electronically stored data used to create in any manner a record or a functional equivalent of a record … will be retained, along with the hardware and software necessary to access the data, for the retention period assigned the record, unless backup copies of the data generated from electronic storage are retained in paper or on microfilm for the retention period." – *Texas State Library and Archives Commission Local Schedules GR and HR, April 3, 2011*