

Policy No.: 2.0802
Page Number: 1 of 17
Effective Date: 04/05/05

TITLE: INFORMATION ASSET SECURITY/USE

PURPOSE: To establish responsibilities and requirements for the protection and proper use of University Health System information assets as they relate to data, image, text and voice objects within internal and external systems by its employees, contractors, and other computer 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 04/01/03. [Key Words: Information Assets, Information System Access, Security, Protected Health Information]

POLICY STATEMENT:

It is the policy of the University Health System to protect the integrity and confidentiality of all information assets while providing access to these assets to appropriately authorized users. The University Health System reserves the right to monitor any and all aspects of the computer system, including electronic mail, files, and internet access, to ensure compliance with this policy. The computer equipment and access given to employees are to assist them in the performance of their jobs. The computer and telecommunication systems belong to University Health System and may be used for business/management approved purposes only. Any item developed and/or created while using this equipment is the property of University Health System.

POLICY ELABORATION:

I. DEFINITIONS:

- A. “Information Assets” include but are not limited to: data, text, image, voice, computers, file servers, workstations, laptops,

software, printers, modems, printed reports, diskettes, CD ROMs, pagers, phones, and internal or external communications networks (Internet, commercial online services, and electronic mail systems) that are accessed directly or indirectly from University Health System's computer facilities.

- B. "Protect" includes preventing misuse, abuse, loss, or unauthorized access or disclosure of information assets.
- C. A "Department Head" is a UHS Department Director or above, who identifies, classifies, creates, maintains, and secures information assets within their areas of responsibility.
- D. A "User" refers to all employees, contractors, and other persons or third parties authorized to access or use University Health System computer or telecommunication or other information assets.
- E. A "Supplier of Information Technology Services" is a provider of information and/or information technology tools (hardware, software, reports, services, etc.) in support of business activities.
- F. "Negligence" the failure to use such care as a reasonably prudent and careful person would do under similar circumstances.
- G. "SPAM E-mail" is an unsolicited commercial message normally sent in bulk.
- H. "Information Services" is a division that consists of Business Applications, Clinical Applications, Technical Services, Operational Services, and HIPAA compliance management.
- I. "Protected Health Information" or PHI means generally, 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; or
3. the past, present or future payment for the provision of health care to an individual.

For the purposes of this policy, an individual such as a Department Head may simultaneously act as a User and/or Department Head, depending on the information used or provided by their department.

II. SCOPE:

This policy is applicable to all information assets and services which support business and clinical activities, and covers all staff, consultants, contractors, and other persons or third parties accessing or using University 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 employment or access to University Health System information assets.

III. RESPONSIBILITIES:

A. DEPARTMENT HEAD:

A "Department Head" is responsible for:

- (1) Knowing the assets and services for which they're

responsible and the applicable control requirements;

- (2) Authorizing Users to utilize information assets and ensuring that these assets are used for management-approved purposes only;
- (3) Assigning custodial authority and responsibility for information asset controls;
- (4) Ensuring effective use of control facilities;
- (5) Ensuring staff education and awareness;
- (6) Responding in a timely, effective way to loss or misuse of information assets and to identified information asset security exposures;
- (7) Conducting assessments for compliance;
- (8) Authorizing access level changes (including access origination, transfers and termination), assigning custody, and authorizing release of information;
- (9) Notifying the Supplier of Information Technology Services of new hires, transfers, terminations and status changes of user accounts;
- (10) Reviewing and updating, at least annually, the list of authorized individuals within the Managers area of responsibility with access to information assets.

B. USER:

A “User” is responsible for:

Policy No.: 2.0802
Page Number: 5 of 17
Effective Date: 04/05/05

1. Complying with information asset security and application system controls as specified by the Supplier of Information Technology Services;
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. Effectively using control facilities and capabilities;
5. Bringing security exposures, misuse or non-compliance situations to management attention;
6. Maintaining confidentiality of information accessed, accessing information that pertains only to their job function.
7. The obligation to maintain the confidential information and security of confidential information continues upon termination of access.

C. SUPPLIER OF INFORMATION TECHNOLOGY SERVICES:

A “Supplier of Information Technology Services” is responsible for:

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

Policy No.: 2.0802
Page Number: 6 of 17
Effective Date: 04/05/05

2. Providing for administration of access to information assets;
3. Providing and administering physical and procedural safeguards for protection of information assets;

4. Effectively communicating installation control facilities, rules and restriction to Users;
5. Providing for timely detection and effective response to unauthorized attempts to gain access to data or restricted areas;
6. Ensuring workstation use is authorized and from authorized locations;
7. Bringing security exposures, misuse, or non-compliance situations to management attention.
8. Establishing security controls and oversight of all UHS software applications to maintain centralized security administration.

IV. GENERAL REQUIREMENTS

- A. Access to University Health System information assets is restricted to authorized individuals and used for business/management approved purposes only. All requests for access must be approved by the department supervisor, Information Services, and the user must sign a confidentiality agreement. Access will be assigned according to users job function.
- B. Users cannot attempt to access or gain access to data that they do not have direct responsibility for or authorization to access.
- C. User ID's follow Information Services standards to maintain consistency across all computing platforms. Generic user ids and

passwords are not permitted as an entry point for any application program. Passwords are set to automatically expire at system defined intervals. Each user is responsible for their user id and password. 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 should attend a basic skills class conducted by Information Services or demonstrate required competency to qualified individuals before being granted access to University 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 University Health System's Information Assets. Users encountering or receiving such material should immediately report the incident to their supervisor and/or the Integrity Office.
- F. Use of the Internet must be in compliance with all University Health System policies, and may not be used for personal financial gain in accordance with University Health System's conflict of interest policy 2.12.
- G. Internet addresses that are deemed inappropriate or non conducive to the work environment are blocked. Internet activity is monitored and recorded.
- 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 Management Team for information asset security compliance before becoming operational in a production environment.
- J. PHI/sensitive information on portable or fixed storage media, (floppy, CD, DVD, etc.), when no longer required, must be deleted or destroyed. All storage media must be destroyed prior to disposal. Cutting the media with scissors is a method of acceptable destruction or you may forward the media to Information Services Security Administration 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. Additional security measures, such as encryption, may be appropriate.
- L. Computers or equipment that connect to University Health System computers or networks, which are not on University Health System premises and not under University Health System control, when used to access University Health System information, must be used for approved management purposes; must be certified for business necessity and interconnection controls and standards by appropriate levels of management to include Information Services, 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 from external sources.

Policy No.: 2.0802
Page Number: 10 of 17
Effective Date: 04/05/05

- M. Software purchased by University Health System is to be used for management 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 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 University 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 UHS facilities are programmed to automatically lock the workstation when the computer receives no input for a specified period of time. The time out period will be limited to 15 minutes or less.
- P. To eliminate or minimize the possibility of unauthorized access to protected health and other confidential information, all University 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 a user leaves their workstation they must either lock the workstation or logoff of the system. Users must logoff at the end

of their shift.

- R. Computing installations and supporting facilities, as determined by management, must be administered as areas of restricted access when continued operation is considered essential or where 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 that can be used to facilitate continuity of operations in the event of an emergency, and recovering from a disaster.
- T. Hardware acquired, installed, added, removed, connected/disconnected, or moved from University Health System infrastructure network or facilities will only be authorized and performed by Information Services. Information Services will maintain an electronic inventory of all computing devices and network hardware.
- U. Protected Health Information may not be transmitted over any communication device unless authorized by Information Services.
- V. No hardware or software applications may be removed from University Health Systems' 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. No food, beverage, or liquid of any kind is to be placed on or near any information asset.
- 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 protected health 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.
- AA. Personal computing devices (laptops, PDA's, etc.) are not permitted to connect to UHS network unless authorized by Information Services.
- BB. The University 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 UHS patients are required to use information systems and other such information assets provided and maintained by UHS. This includes physicians, nurses, and all others as defined in this policy.

V. 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 University 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. University 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.
- F. University Health System will utilize software to automatically block any Spam E-mail.
- G. E-mail that is sent internal to University 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 their designee, Corporate Communications, and the Vice President of Information Services or their designee.
- H. All E-mail sent via the internet containing PHI must be encrypted.

Policy No.: 2.0802
Page Number: 14 of 17
Effective Date: 04/05/05

To encrypt an E-mail, type "PHI:" anywhere in the subject line.

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

VI. FACSIMILE REQUIREMENTS

- A. Transmission of protected health information via facsimile is restricted to information required for continuity of care where other means of delivery are not appropriate.
- B. All facsimiles must be accompanied by University Health System approved cover sheets (provided on the UHS 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 protected health information 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. A "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 protected health information.
- E. Protected Health Information 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. PBX security software is installed on all University Health System phone switches. This software is used to monitor, secure and track call activity.
- B. Area codes 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 University Health System; however discretion must be used to ensure patient care is not disrupted or compromised. The use of camera phones for the purpose of taking pictures is prohibited on UHS property without proper authorization. See Patient's Right to Consent, Policy No. 9.02.
- E. Users are prohibited from connecting modems of any type to the University 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 University Health System communications infrastructure. Requests for phones must be approved and installed by

Information Services.

- G. Patient and confidential information may be left on voicemail only if you can verify voicemail is being used and not an answering machine, otherwise a call back number is to be left where you can be reached. Patient and confidential information must not be left on answering machines.
- H. In order to prevent unnecessary costs to Health System, users should not use 1411 for information. A phone directory is available online that contains the Yellow, White, and Business pages for San Antonio and surrounding areas. Phone books are also available.
- I. University 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 shall immediately report the incident to their supervisor and/or the Integrity Office. Information Services should be notified immediately in incidents where assets are at risk. It is the responsibility of the supervisor to notify 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/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 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.

Policy No.: 2.0802
Page Number: 17 of 17
Effective Date: 04/05/05

REFERENCES/BIBLIOGRAPHY:

UHS Conflict of Interest Policy, No. 2.12

UHS HIPAA Compliance Policy, No. 2.14

UHS Reporting Errors and Incidents of Misconduct Policy, No. 2.13

UHS Medical Records Policy, No. 10.03

Patient's Right to Consent Policy, No. 9.02

Information Security Policies Made Easy, Charles Wood, PentaSafe, 2003

Corporate Internet, Intranet and E-mail Policies, New York Law Journal, Internet, 2000

Society for Human Resource Management, Internet, 1998

UHS Information Services Standards Manual, 2004

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

IT Governance Institute Control Objectives, 2000

OFFICE OF PRIMARY RESPONSIBILITY: Information Services