University Physicians Inc.

SAFEGUARDS POLICY

Latest Revision:
Original Effective Date: April 4, 2003

Purpose

To maintain appropriate **administrative**, **technical**, and **physical** safeguards to protect the confidentiality, integrity and availability of PHI pursuant to HIPAA standards.

Policy

This policy applies to all PHI existing in either electronic or paper form that is physically housed at UPI or otherwise managed under the direction of UPI organizational units or individuals.

This policy has been developed in coordination with UPI's Affiliates. Accountability for complying with HIPAA regulations applies to everyone in the UPI organization. Efforts to safeguard PHI are expected to be appropriate to the situation and reasonable in regard to effort and expense.

The direct responsibility of maintaining compliance with this policy resides with all UPI employees and any other individual with access to UPI's computer systems.

Penalties and disciplinary actions will arise from non-compliance with HIPAA policies after appropriate HIPAA educational activities have taken place and if remediation of reoccurring issues has failed.

This policy describes UPI's expectations in the areas of administrative, technical, and physical safeguards. The HIPAA Privacy Rule provides some specifics regarding what the Federal Government requires in the area of safeguarding PHI. The HIPAA Security Rule was published on February 20, 2003. This policy will be revised and reissued in the near future to reflect any additional requirements.

The HIPAA Privacy Rule 164.530(c) requires that covered entities reasonably safeguard protected health information to limit incidental uses or disclosures.

Procedure

A. Administrative

Computer software applications containing PHI are to be registered with the UPI HIPAA Privacy Officer for the purpose of building an institutional PHI inventory.

Organizational units or individuals administratively responsible for handling PHI are expected to keep their processes and practices in compliance with UPI HIPAA policies.

Non-compliance issues may be reported to **hipaa@upicolo.org**. The UPI HIPAA Privacy Officer and Security Officers will review issues brought to their attention regarding non-compliance and assist, where possible, with remediation efforts.

All UPI systems and equipment are subject to compliance inspections. Spot audits and inspections will be performed.

B. Technical

Technical aspects associated with ensuring the privacy of PHI in some cases will require the expertise of information technology professionals. In these situations responsibility for ensuring the privacy of PHI will be shared jointly by the end users and the UPI Information Services (IS) Department.

End User Responsibilities

Account access. Every individual must have a personal login (or username) and password for authorization and authentication prior to accessing UPI's computer systems. Passwords must not be disclosed to anyone, including co-workers, managers, or IS support representatives. Usernames should not be shared or included in published employee lists.

The use of hardened passwords is required, when allowed by the system. Guidelines for hardening passwords and other password policy information may be found on the UPI shared drive at S:/UPI/Save/ISPolicies. Users must log out of or "lock" their computer systems when not in use to reduce the risk of improper access to PHI.

Desktop computers. PHI should not be stored on the hard drive of desktop computers. Placing PHI on the hard drive of a desktop computer raises the security requirements for that desktop to the level of a server containing PHI. It is easier to physically protect a limited number of servers than to protect every end user's desktop. It is strongly recommended that all PHI be stored on either a user's P:/ drive or on the S:/ drive in a secure folder.

Screen savers must be enabled and password protected so that screen displays are masked after no more than five minutes of inactivity and to ensure that a password is required before the display can be reactivated. If use of a shared computer is required, each end user must log off the system prior to relinquishing the computer to the next user.

Email. If PHI must be transmitted via email and the email recipient is part of the internal email system (i.e. UCHSC, UCH, or UPI), the email does not need to be encrypted, given the network is private. If the email must be sent across the

Internet, encryption should be applied to the email message. Please contact the UPI IS Department for assistance with email encryption.

Personal email accounts must never be used to transmit email containing PHI, because these email systems are not encrypted.

Fax Machines. Fax machines used for transmitting or receiving PHI must be in locations secured from the general public. Before sending faxes, ensure that the destination phone number is correct and that the fax cover sheet includes UPI's standard disclaimer notice. Faxes should always have cover sheets.

Portable computing devices. Portable computing devices include electronic devices ranging from laptops to personal digital assistants (PDA). Given their small size and portability, loss or theft is a constant possibility.

The best practice is to keep sensitive information off such devices entirely. Failing that, devices must be password protected and, where possible, the PHI data on the devices encrypted. Please contact the UPI IS Department for assistance with encryption.

Physical security is critical. End users and departments are responsible for keeping track of PDAs, laptops, and other mobile devices. If the portable computing device is lost or stolen, the user of that device is responsible for immediately notifying his or her department and the UPI HIPAA Privacy Officer. This requirement applies to both company-owned and personal equipment.

Providing Internet access to PHI. Since the Internet is inherently insecure and there is a risk of data being intercepted, PHI should not be transmitted over the Internet, including Internet email, unless the data is encrypted. Industry-accepted methods of encrypting Internet traffic include, but are not limited to, secure sockets layer (SSL) encryption, virtual private networking (VPN), secure Citrix software, and secure shell (SSH). Please contact the UPI IS Department for assistance with secure Internet transmissions.

Remote access. Individuals accessing UPI's computer systems via remote access have a responsibility to operate and maintain current anti-virus software at their remote locations. Software security patches must also be maintained. Users of Digital Subscriber Lines (DSL) or cable modem services are required to operate VPN software and personal firewall software in addition to anti-virus software to mitigate the increased risks posed by these high-speed connections. The UPI IS Department will install and maintain software required for remote access on equipment owned by the company. IS will assist individuals in the implementation of remote access requirements for personal equipment. The user must be able to bring in their computer for updates on an as-required basis. The UPI IS Department reserves the right to verify that protections are in place.

Wireless network devices. Wireless network devices use radio frequency transmissions to replace wire connections. Signals broadcast by wireless devices can travel far beyond the confines of any structure. For this reason wireless network devices are not currently permitted at UPI.

UPI IS Department Responsibilities

The UPI IS Department will periodically scan and review both systems and devices

to ensure that safeguards are in place.

The UPI IS Department will notify the UPI HIPAA Privacy and Security Officers immediately if it finds that a system does not have the appropriate safeguards.

Access controls. Access to UPI's computer systems shall only be granted after the UPI IS Department has completed an account creation process. Components of an account creation process include completion of a UPI User Account Security form, positive identification of the individual, documentation of the person's roles and access requirements, education of the individual regarding proper use of the account, and written acceptance of UPI's policies regarding appropriate use of its computer resources. The UPI User Account Security form and completion instructions may be downloaded from the UPI web site at http://upi.uchsc.edu/is.html.

Modifications to established accounts require documentation of the individual's new roles and access requirements and, in some cases, the submission of an updated UPI User Account Security form.

Where feasible, access to PHI will be limited to the minimum necessary to fulfill that person's work obligations.

All computer systems and applications shall be administered, where possible, to adhere to the password standards found on the UPI shared drive at S:/UPI/Save/ISPolicies.

Audit trails. Audit trails can be used to trace suspicious patterns of use and as a backup to the limitations that access controls provide. Where computer system capabilities allow it, audit trails to activities performed on a system should be created. The IS Department shall review audit records on a routine basis.

Change control management. The processes by which software is developed, installed, and maintained should be given specific attention. Reasonable and appropriate methods will vary based on the type of system involved and the nature of the data.

Security patches/virus control. All computers attached to the UPI network will operate and maintain current anti-virus software. Security patches for software and operating systems shall also be maintained.

C. Physical

It is natural to focus on technical aspects of security, but physical protections are critical too. The following safeguards are strongly recommended to physically protect PHI:

- Restrict access to areas with printed materials, fax machines, or computers containing PHI.
- Keep such areas secured after hours and when otherwise not in use.
- Secure printed materials containing PHI.
- Remove printed materials containing PHI from copy machines, printers, or fax machines.

- When not in use, secure portable storage media (i.e. removable drives, diskettes, CDs, tapes, etc.) or portable computing devices containing PHI.
- When no longer needed, ensure that any printed material is shredded and portable storage devices containing PHI are properly erased or destroyed.

Neglect of physical security leads to security problems. Even the most sophisticated electronic security efforts can be defeated by inattention to the basics of physical security.

Definitions

See glossary for key terms and acronyms used in this policy (on file with the Privacy Officer).

Encryption – the conversion of data into a form unreadable by anyone without a secret deciphering/decryption key.

Software security patch – a quick-repair job (sometimes called a "fix") for a computer program that specifically fixes a problem that, if not fixed, could lead to a security breach.

Enforcement

Enforcement of this policy will reside with the Privacy and Security Officers or appropriate Management.

Rationale/ Source

This policy complies with requirements of the following:
Health Insurance Portability and Accountability Act (HIPAA), Privacy Rule

---

Cross References

For additional information, refer to the following:

Document Name

Review or Revision Date

This policy is reviewed and approved annually and as revised.

MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY

Governance Responsibility for adoption and/or implementation of this policy is as follows:

Approving Body			
Privacy Officer: **Signature on file.**	**04/04/03** **Date**	**Security Officer:** **Signature on file.**	**04/04/03** **Date**
Executive Approval			
Chief Operating Officer: **Signature on file.**		**04/04/03** **Date**	