Section 8.3: Safeguarding PHI	**Page:** 1 of 4
Effective Date: September 23, 2013	

POLICY

System shall safeguard PHI so as to minimize Uses and Disclosures of PHI that violate the HIPAA Privacy Standards or the policies and procedures set forth in this Manual.

8.3(1) Written Documents

a. Papers containing PHI shall be picked up as soon as reasonably possible from publicly accessible locations, such as copiers, mailboxes, and conference room tables, and shall be appropriately filed or destroyed. PHI shall not be left unattended unless the area is secured from unauthorized access.

b. Offices and file cabinets in common areas containing PHI shall be locked during hours when the office is closed and only persons authorized to access the PHI shall be able to unlock the offices or file cabinets.

c. Documents containing PHI shall not be discarded in trash bins, recycling bins, or any publicly accessible locations. All discarded PHI shall be placed in a secure bin for secure disposal. Microfilm and microfiche shall be cut into pieces or chemically destroyed. Any other media containing PHI shall be destroyed such that the PHI cannot be read or accessed before it is discarded.

d. PHI in paper form shall not be removed from an office by staff or other Workforce Members except when Use of the PHI is required for official business. Such PHI should be under the direct control of the person conducting the business that requires its removal and Use at tall times, maintained securely at all times by the person, and returned to the office from which it was removed without delay by the person.

8.3(2) Electronic PHI

a. All System computers and other devices on which electronic PHI is created or maintained must be encrypted in compliance with System policies.

b. Passwords to computers and other devices upon which PHI is maintained or created shall not be shared by staff or other Workforce Members and shall not be written down where others can find them. A computer user with access to PHI via the computer shall log off or use a password protected screen saver

before leaving his or her workstation for any significant period of time and shall not allow someone else to use his or her computer under his or her password in his or her absence.

b. A computer screen or other device screen shall not be positioned such that PHI may be viewed by unauthorized individuals.

c. Copiers and other devices capable of caching PHI should be cleared of all PHI prior to removal from an office within the Health Care Component.

d. Before new technologies or devices are adopted or obtained by an office within the Health Care Component, that office and other System offices involved in the adoption or acquisition of the technology or device are responsible for determining if PHI is reasonably likely to be created or maintained as the result of the adoption or acquisition and policies and procedures must be adopted for ensuring the security of all PHI created or maintained or Used or Disclosed as a result. This applies to Social Media sites, messaging systems, and smart phone or other PDA applications that an office sponsors or utilizes.

e. Offices should discourage the use of personal devices, such as laptops, phones, personal devices for the creation or storage of PHI in any form, including texts. If PHI is created or maintained on such devices, the office must require that the staff or workforce member that creates or maintains the PHI on the device ensures that the device is encrypted in compliance with System requirements and all PHI is subsequently either transferred to a secure System owned or controlled information resource, or securely destroyed, without delay.

8.3(3) Mailing PHI

Records containing PHI, if mailed, should be sent in a sealed envelope marked "CONFIDENTIAL."

8.4(4) Emailing PHI

Emails containing PHI in transit and in storage by or on behalf of System must be encrypted. If an Individual requests that PHI be emailed to them or on their behalf where encryption is not possible, the Individual should be advised of the risk of access of the PHI by unauthorized person and should affirmatively consent to the risk before the PHI is emailed.

8.3(4) Faxing PHI

a. All pages of a facsimile containing PHI shall be marked "CONFIDENTIAL." The facsimile cover letter shall contain a notice of disclosure that informs the recipient that the information is confidential, identifies the proper recipient, and directs any other person who receives the fax to notify the sender immediately of the error.

b. To help ensure that faxes are sent to the correct destination, any frequently used numbers or programmed numbers shall be periodically checked for accuracy, and new fax numbers shall be verified with the intended recipient before any PHI is faxed.

c. If System learns that a fax has been misdirected, the recipient shall be reached by phone or by fax and instructed to destroy the misdirected fax.

8.3(5) Verbal Communications

System shall reasonably safeguard PHI that is orally Used or Disclosed in order to limit incidental Uses and Disclosures of the PHI. Conversations, whether face-to-face or by telephone, that involve PHI should be conducted in private (e.g., behind closed doors) or spoken softly, without excessive use of the subject's name.

8.3(6) Electronic Storage of PHI

a. System shall reasonably safeguard PHI that is electronically stored in order to limit incidental Uses and Disclosures of PHI. Electronically stored PHI may be located on The University of Texas at Austin administrative mainframe, System servers or network attached storage devices, PC workstations, on System Administration's Office of Information Resources servers or network attached storage devices, or, on electronic storage media such as cartridge tapes, compact disks, or floppy discs.

b. Electronic PHI stored by EGI in accordance with paragraph (a) on any computer system or storage device shall be encrypted whenever feasible and protected by User ID and Password protection. Electronic media containing PHI that cannot be password protected shall be secured in locked cabinets or closets to which only Workforce Staff authorized to access the PHI have access.

8.3(7) Separation of Group Health Plan Records from Employee and other Non-Group Health Plan Information

a. OEB shall keep all records concerning Group Health Plans containing PHI separate from other Non-Group Health Plan Information including employment-related information kept by OEB and/or The System.

b. PHI held by OEB shall not be Used or Disclosed in connection with any Non-Group Health Plan functions including employment-related functions performed by OEB and/or The System without an Authorization permitting the Use or Disclosure or under an exception permitted by this Manual and the Privacy Rules.

REFERENCES/CITATIONS

45 C.F.R. § 164.530(c)

65 Fed. Reg. at 82,561-62, 82,745-46 (Dec. 28, 2000); 67 Fed. Reg. at 53,193-95 (Aug. 14, 2002)