**UNIVERSITY OF OKLAHOMA**

###  **HIPAA Privacy Policies**

|  |  |
| --- | --- |
| **Subject:** Safeguards  | **Page:** 1 of 7 |
| **Policy #:** Privacy-18 (Admin.)  | **Approved:** August 4, 2008 |
| **Effective Date:** August 5, 2008 | **Last Revised:** 2/1/16; 6/15/16; 2/27/17; 5/19/17 |

## **I. PURPOSE**

To establish minimum safeguards that must be implemented by the University’s Health Care Components to protect Protected Health Information.

**II. POLICY\***

The University, through its Health Care Components, will implement appropriate administrative, technical, and physical safeguards that will reasonably protect Protected Health Information (PHI) from any intentional or unintentional Use or Disclosure that is in violation of the University’s Privacy and Security Policies and the Privacy or Security Regulations and limit incidental Uses and Disclosures of PHI.

**Workforce Members must reasonably safeguard PHI to limit incidental Uses and Disclosures made pursuant to an otherwise permitted or required Use or Disclosure.**

**Health Care Components may Disclose PHI to other components of the University that are not designated Health Care Components only with patient Authorization or as permitted or Required by Law. University Personnel who perform services for Health Care Components and other components of the University must not otherwise Use or Disclose PHI created or received in the course of or incident to their work for the Health Care Component to components of the University that are not Health Care Components.**

####

This policy establishes minimum administrative and physical standards regarding the protection of PHI that each Health Care Component must enforce, as applicable. Health Care Components may develop additional policies and procedures that are stricter than the those set forth in this Policy to address the unique circumstances of a particular Health Care Component. Policies and procedures developed in addition to those stated herein will be reviewed by the University’s Privacy Official and Security Officer upon request.

**Technical safeguards regarding the protection of PHI maintained in electronic form are available from Information Technology and the University HIPAA Security Officer. Some are incorporated into this Policy by reference.**

#### A. Administrative Safeguards.

1. Oral Communications. University Personnel must exercise due care to avoid unnecessary Disclosures of PHI through oral communications. Voices should be quiet and conversation should not occur if unauthorized individuals are present. Patient identifying information should be Disclosed during oral conversations only when necessary for Treatment, Payment, teaching, Research, or Healthcare Operations purposes. Dictation and telephone conversations must be conducted away from public areas if possible. Office doors should be closed when PHI is being discussed. Speakerphones may be used only in private areas.

1. Telephone Messages. Telephone messages and appointment reminders that do not contain PHI may be left on answering machines and voice mail systems, unless the patient has requested and received approval for an alternative means of communication (See Privacy-07, Communication by Alternative Means.) Telephone messages that contain information that links a patient to a particular medical condition, diagnosis, or treatment must be avoided.

Acceptable: This is John calling from OU Physicians to confirm an appointment.

Not Acceptable: This is John calling from the Pediatric Oncology clinic to confirm an appointment.

1. Faxes. The following procedures must be followed when faxing PHI:

1. Each Health Care Component must provide training on this section to Workforce Members who will fax, or approve the faxing of, PHI
2. Only the PHI necessary to meet the authorized requester’s needs may be faxed.
3. Unless otherwise permitted or Required by Law, a properly completed and signed Authorization must be obtained before faxing PHI to third parties (including faxes to University departments that are not designated Health Care Components) for purposes other than Treatment, Payment, or Health Care Operations. (See Privacy-23, Authorization.)
4. All faxes containing PHI must be accompanied by a cover sheet that includes a confidentiality notice. PHI may not be included on the cover sheet. A sample fax cover sheet with the confidentiality notice is available on the HIPAA Forms webpage.
5. Reasonable efforts must be made to ensure that fax transmissions are sent to the correct destination. Frequently used numbers should be programmed into fax machines or computers to avoid dialing errors. Programmed numbers should be verified on a regular basis. The numbers of new recipients should be verified prior to transmission.
6. Fax machines must be located in attended areas or in secure areas not readily accessible to visitors or patients to protect incoming and outgoing PHI. Faxes containing PHI must not be left sitting on or near the machine for extended periods of time.

1. Fax confirmation sheets shall be reviewed to ensure the intended destination matches the number on the confirmation sheet, if available. The confirmation sheet shall be attached to and maintained with the document that was faxed.
2. All instances of misdirected faxes containing PHI must be reported to the University Privacy Official, investigated, and mitigated pursuant to Privacy-13, Complaint Reporting and Tracking; Privacy-14, Mitigation; Privacy-06, Accounting of Disclosures; and any internal Health Care Component reporting requirements.
3. Mail. PHI may be mailed within the University if placed in sealed envelopes or in locked mail bags. PHI, including appointment reminders, may be mailed outside the University if the contents are concealed and the envelope is sealed.
4. Copies. All copies of PHI provided to the patient or another third party in response to a request for access should be date stamped in a color other than black or should bear some other unique identifying mark or symbol, so that a copy can be distinguished from the original.

**Date stamping or marking records provided to patients will protect the University in the event there is a dispute as to how or when certain records were acquired or Disclosed.**

1. Sign-in Sheets. Sign-in sheets in departments or clinics that primarily see and treat patients with mental health, substance abuse, communicable disease, or other particularly sensitive conditions must be structured in a manner so that subsequent signers cannot identify previous signers. No sign-in sheets in any department or clinic may require patients to disclose PHI beyond their names.

1. Destruction Standards. PHI must be discarded in a manner that protects the confidentiality of such information. Paper and other printed materials containing PHI shall be destroyed or cross-cut shredded so that they cannot be read or reconstructed. Health Care Components may also obtain and use locked recycling bins from one of the University’s approved recycling vendors. Magnetic media and diskettes containing PHI shall be overwritten, reformatted, or destroyed pursuant to industry standards (available from IT Security.) Hard drives and other electronic devices shall be destroyed or managed in accordance with applicable Security and HIPAA Security policies.

B. Physical Safeguards.

1. Paper Records. Documents containing PHI must be stored or filed in such a way as to avoid access by unauthorized persons. Some type of reasonable physical barrier must be used to protect paper records from unauthorized access. Documents containing PHI on attended desks, counters, or nurses’ stations must be placed face down or positioned in a manner that prevents access by unauthorized persons. Paper records shall be secured when the area is unattended.
2. Storage. Paper records that contain PHI and are stored outside of the Health Care Component must be inventoried and stored in a secure, University-approved facility. The Health Care Component shall maintain a log of who has access to the stored records and have in place a procedure for terminating access when employment ends. (See Procedures for Storing Protected Health Information on the HIPAA FAQ page.)

1. Removal. **Workforce Members shall not remove documents containing PHI from the University premises solely for their convenience.** Workforce Members may remove such documents from University premises when necessary for Treatment, Payment, or Operations or Required by Law. Any such documents that must be removed from University premises shall be checked out according to applicable Health Care Component policies or procedures, which must be in writing, and must be returned as soon as they are no longer needed for that purpose. The security and return of the documents checked out or removed are the sole responsibility of the person who removed them.

Documents containing PHI that are removed from University premises must not be left unattended in places in which unauthorized persons can gain access, legally or otherwise. They must not be left unattended in the passenger compartment of automobiles, for example, or in common areas.

1. Escorting Visitors and Patients. To ensure they do not have unauthorized access to PHI, during business hours, visitors and patients must be escorted and/or monitored when on University premises where PHI is located or where patients are being seen. After hours access must be escorted or monitored, as appropriate based on the premises and the PHI stored on the premises.

**Persons who are not employed by the Health Care Component, including but not limited to pharmaceutical representatives and service providers, shall not be in areas in where patients are being seen or where PHI is located, without appropriate supervision.**

3. Computer/Work Stations. Computer monitors must be protected from view, positioned away from common areas, or covered by a privacy screen to prevent unauthorized observation of PHI. The screens on computers must be returned to a password-protected screen saver or login screen when the computers will be unattended. If PHI must be stored on the actual workstation (rather than on a secure server, as recommended), the work station must be encrypted.

4. Equipment. Equipment containing PHI (e.g., desktop computers, medical equipment, fax machines, monitors) must be physically and/or technically secured, as appropriate, when not attended, such as by encryption for portable devices or by physical security features (e.g., alarms, locks) for copiers and scanners. University-owned and University-leased equipment that contains PHI may not be removed from University premises without supervisor approval. The security and return of the equipment are the sole responsibility of the person who removed the equipment, as described in Section B (1)(b) above. The removal must be consistent with applicable University or Health Care Component policy, which may require completion of a property control or inventory check-out form, and must be recorded on the Health Care Component’s device and equipment inventory, as described in the HIPAA Security Device and Media Controls policy.

C. Technical Safeguards.

1. Telemedicine Technology. The use of Telemedicine Technology must meet all Safeguards, as specified in the HIPAA Privacy and Security Policies, and the AES Encryption standards for H.323 protocol communications. IT Security must be contacted for additional information.
2. E-mail Within the University. Sending e-mails that contain PHI for Treatment, Payment, or Health Care Operations within the University (OUHSC.edu/OU.edu to OUHSC.edu/ou.edu) is acceptable. PHI should be sent as a limited data set when possible. The minimum necessary standard (See Privacy–21, Minimum Necessary Rule) must be observed when applicable.
3. E-mail Between OUHSC.EDU and HCAHealthcare.com E-mail Addresses. Sending e-mails that contain PHI for Treatment, Payment, or Health Care Operations between ouhsc.edu and HCAHealthcare.com email addresses is secure and therefore acceptable. PHI sent should be sent as a limited data set when possible and in accordance with the Minimum Necessary Rule, as applicable.
4. E-mail Outside the University. E-mail may be used to transmit PHI to an authorized recipient outside the University only for Treatment, Payment, or Health Care Operations or to University Business Associates. The message must be encrypted between sender and recipient in a manner that complies with HIPAA. See the IT Security Secure Email Page (<http://it.ouhsc.edu/services/infosecurity/SecureEmail.asp>) for a list of entities with which OUHSC IT has established an encrypted (TLS) channel. If an encrypted channel does not exist, other options for secure transmissions include, for example, emailing from the EMR, through a secure patient portal, or typing in the subject line **[secure]** for Health Sciences Center email accounts or **[OUENCRYPT]** for Norman Campus email accounts, if available. No PHI may be included in the subject line of any email message.

Employees of Health Care components may not auto-forward email to a non-OUHSC.edu or non-OU.edu email address. Each Health Care Component shall have in place procedures for emailing PHI.

# When E-mail Encryption is Available. Subject to the Health Care Component’s internal policies and procedures, University Personnel may send PHI via encrypted email for Treatment, Payment, or Health Care Operations or to University Business Associates.

# Without Encryption Capabilities (E-Mail Communication Denial). If a patient sends an e-mail to an employee, student/trainee, or volunteer asking a health care question or requesting any type of information that would require a Disclosure of PHI, the request for response shall be declined by sending a new message similar to the following:

“I have received your health care question or request for health information. However, I cannot respond using e-mail because to do so would require the transmission of information that I consider to be highly sensitive, and e-mails can be intercepted easily. I will respond to your question or request through some other means of communication. If you wish to receive health information via email, please submit Consent for Electronic Communication form to your health care provider or log in to your patient portal account, if available.”

**Note: The Consent for Electronic Communication form is available on the HIPAA forms webpage.**

If a patient does not want to complete this form but insists on receiving PHI via unsecure email, University Personnel shall refer to their Health Care Component email procedure or refer the patient to the supervisor. The supervisor shall obtain written confirmation from the patient that the patient understands that the email will not be secure and may be intercepted by an unauthorized individual, but still wishes to receive the PHI via mail. The patient’s written confirmation must be maintained in the patient’s file for six (6) years.

1. **Email Notice. All e-mails containing PHI transmitted by Health Care Components must contain a Confidentiality Notice similar to the following:**

*This e-mail, including any attachments, contains information that may be confidential or privileged. The information is intended to be for the use of the individual or entity named above. If you are not the intended recipient, be aware that any disclosure, copying, distribution, or use of the contents is prohibited.*

*If you have received this e-mail in error, please notify the sender immediately by a “reply to sender only” message and destroy all electronic and hard copies of the communication, including attachments.*

1. Electronic Documents. Documents and attachments and/or images containing PHI are expected to be stored on network servers with appropriate security restrictions in accordance with IT Security policy, rather than about portable devices or unsecure desktop computers. (IT Security can provide specific information on these servers.) If documents and attachments and/or images cannot be stored on such a network server but instead are stored on a desktop computer or portable computer device, the workforce member must ensure that the computer or device is encrypted by contacting the appropriate IT representative.
2. Portable Computing Devices (e.g., laptops, smart phones, tablets, flash drives) and Desktops. Employees, volunteers, and students/trainees must use extreme caution when using Portable Computing Devices and desktop computers to store PHI. PHI should not be stored on Portable Computing Devices and desktop computers unless absolutely necessary; it should be stored on servers in a secure enterprise data center, as described in Paragraph 6 above. If PHI is stored on such devices or computers, the device or computer must be encrypted pursuant to HIPAA Security policies and applicable University policies. Portable Computing Devices must never be left unattended in unsecured places.

The failure to take the above security precautions will be considered a violation of these Policies, subjecting the user to sanctions.

Volunteers, except for volunteer faculty, are not authorized to store PHI on personal portable devices.

**NOTE: The Office for Civil Rights has stated that it considers storing PHI on unencrypted portable devices to be an act of deliberate indifference with regard to the protection of PHI.** Contact IT Security or the HIPAA Security Officer if you believe you have circumstances that warrant special encryption consideration.

1. Other Uses/Internet. Any other electronic transmission of PHI requires that appropriate safeguards and procedures be implemented. Health Care Components and Workforce Members should contact IT Security or the HIPAA Security Officer for more information.
2. Social Media Sites. Protected Health Information shall not be posted on social media sites, such as Facebook or Twitter. University Personnel should keep in mind that even if a patient’s name is not posted, if the patient could reasonably be identified, alone or with information obtained from other sources, the information is considered Protected Health Information.
3. Digital Copiers/Scanners. Health Care Components using digital copiers, scanners, fax machines, and other equipment that stores PHI, even temporarily, must verify that appropriate data security features (e.g., encryption, overwriting) are enabled. In addition, before such equipment is returned to the vendor, transferred, surplussed, or otherwise disposed of, the Health Care Component must take steps to ensure the hard drive is destroyed or completely overwritten. These steps may include, but are not limited to, notifying the Purchasing Department to impose these requirements on the vendor during the contracting process or working with IT Security prior to retiring, disposing of, transferring, or surplussing the device to ensure the PHI is removed. (See Privacy-33, Purchasing or Leasing Equipment.)

Health Care Components should have a Service Level Agreement in place with IT if any of these steps are delegated to IT or another University Department.

D. Theft or Loss. The theft or loss of any document, electronic medical record, or device containing Protected Health Information (including those owned by the individual) shall be reported immediately to the University Privacy Official and HIPAA Security Officer, as appropriate, and any person designated by the Health Care Component so that mitigation and reporting options can be considered and implemented as soon as possible. (See Privacy-34, Security Breaches). Report to Local Law Enforcement is expected in case of theft.

## **III. REFERENCES**

#### HIPAA Privacy Regulations, 45 CFR §164.530.

1. OUHSC Property Inventory § 581 (B)(2) and Equipment Inventory Off-Campus Usage Authorization Form, each as revised.
2. Norman Campus Property Control, Temporary Equipment Use Agreement, as revised.