UNIVERSITY OF OKLAHOMA

HIPAA Policies

Title: Safeguards - Administrative and Physical	**Approved:** August 4, 2008
Effective Date: August 5, 2008	**Last Revised:** 4/1/18; 12/18/18, 2/15/19

I. PURPOSE

To establish minimum administrative and physical 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 and physical safeguards that will reasonably protect Protected Health Information (PHI) from any intentional or unintentional Use or Disclosure that is in violation of HIPAA and the University's HIPAA Policies and limit incidental Uses and Disclosures of PHI.

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 in this Policy to address the unique circumstances of a particular Health Care Component but may not do less than is required by this policy. Policies and procedures developed in addition to these will be reviewed by the University's Privacy Official and Security Officer upon request.

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

B. Health Care Components may Disclose PHI to other components of the University or campus Covered Entities 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 for 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.

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

*Capitalized terms are defined in HIPAA *Definitions* policy

NOTE: Clinical work performed by dually-employed Workforce Members at the affiliated institution, OU Medicine, Inc. (d/b/a OU Health and OU Health Physicians) must be done in compliance with OU Medicine, Inc. (d/b/a OU Health and OU Health Physicians) policies and procedures.

A. Administrative Safeguards.

1. Oral Communications. University Personnel must exercise care to avoid unnecessary Disclosures of PHI during oral communications. For example, 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 In emergency situations, Workforce Members may engage in communications as required for quick, effective, and high quality health care.. When appropriate and practicable, suggested safeguard examples include, but are not limited to:

   a. Using lowered voices;
   b. Closing the curtain in semi-private rooms;
   c. Speaking away from others;
   d. Refraining from discussing PHI in elevators, cafeterias, or other public areas; and
   e. Asking visitors to leave the room or obtaining patient consent prior to speaking in front of visitors.

2. 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 HIPAA *Communication by Alternative Means* policy.) Telephone messages that contain information that links a patient to a particular medical condition, diagnosis, or treatment must be avoided, unless the patient has provided written Authorization to receive PHI in telephone messages.

   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 for chemotherapy.

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

   a. Each Health Care Component must provide training on faxing PHI to Workforce Members who will fax, or approve the faxing of, PHI.

   b. Only the PHI necessary to meet the authorized recipient's needs may be faxed.

   c. 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 HIPAA *Authorization to Use or Disclose PHI – Other Than to Patient* policy.)

d. 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.

e. 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 or stored fax numbers must be verified on a regular basis. The numbers of new recipients should be verified prior to first transmission.

f. 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. If a HCC is utilizing an e-faxing system, the HCC should ensure it has been reviewed by IT Security prior to use, and that the e-faxes should be sent to a secure location and minimum necessary access to the receiving location is observed.

g. Fax confirmation sheets should be reviewed to ensure the intended destination matches the number on the confirmation sheet, if available. The confirmation sheet should be maintained with the document that was faxed.

h. All instances of misdirected faxes containing PHI must be reported to the University Privacy Official or HIPAA Security Officer, investigated, and mitigated pursuant to the HIPAA *Complaint Reporting and Tracking*; *Mitigation*; and *Accounting of Disclosures* policies, as well as any internal Health Care Component reporting requirements.

When faxing PHI, workforce members should take appropriate safeguards:

1. Locate fax machines in low-traffic areas and inaccessible to visitors.
2. Consider whether it is appropriate to fax the PHI (*e.g.*, is there another secure method to send the information, is the recipient authorized to receive the information, is the PHI particularly "sensitive").
3. If possible, confirm the recipient is available by calling them prior to sending the fax.
4. Verify the fax number before sending.
5. Use the HIPAA fax coversheet (do not include PHI on the cover page).
6. Double check the fax number entered before sending.
7. Set the fax machine to print an auto-confirmation page, if available, and check the confirmation page to ensure:
    A. Delivery was successful, and
    B. Correct fax number was dialed
8. Use pre-programmed fax numbers, if available
    A. Test pre-programmed fax numbers prior to use.
    B. Have a process in place to verify the programmed numbers on a regular basis.
    C. Remind regular fax recipients to provide updated fax numbers when numbers change.

4. Mail. PHI may be mailed within the University if placed in a sealed envelope or in a locked mail bag. PHI, including appointment reminders, may be mailed outside the University if the contents are concealed and the envelope is sealed. Reasonable efforts must be made to ensure that mail is sent to the correct destination and senders should review the mailing address prior to sending. The return address may not indicate the nature of diagnosis, treatment, or condition.

Mail and package delivery (e.g., US Postal Service, Fed Ex) pick-up sites should be in a separate location from employee desks or customer counters to help avoid the wrong information being picked up.

5. Copies and Print-outs. All copies and print-outs 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 have some other unique identifying mark or symbol, so that a copy can be distinguished from the original. Reasonable efforts must be made to ensure that the correct patient information is given prior to handing the document to the patient or another third party by verifying the patient's name on the document. HCCs must have a process in place to verify documents are for the correct patient prior to providing the documents to the recipient (*e.g.*, verify recipient by highlighting the patients name prior to giving discharge papers to an individual).

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.

6. 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.

7. Destruction Standards. PHI must be discarded in a manner that protects the Confidentiality of the information. Paper and other printed materials containing PHI must 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 disks containing PHI must be overwritten or reformatted if possible or shredded or otherwise destroyed pursuant to industry standards (available from IT Security.) Hard drives and other electronic devices must be destroyed or managed in accordance with applicable IT Security policies. (Additional information is available from IT Representatives/ Tier 1s.)

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 secure 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 even for a brief moment.

a. 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.)

b. 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 as Required by Law. Any documents that must be removed from University premises must be checked out according to applicable Health Care Component procedures, which must be in writing, and must be returned as soon as they are no longer needed for that purpose. Health Care Components that require a routine removal of PHI (i.e. schedule lists, batch reports, case log books) must have a documented procedure for the routine removal of the PHI that outlines what is permissible and the expectations to Safeguard the PHI.

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, an unlocked vehicle, or a locked vehicle in which the PHI is in plain view or is held in a visible container that may encourage theft such as a box of records, a briefcase, or a laptop computer case.

c. Off Premises Developed Documents. If a Workforce Member is conducting University Business off the University premises and develops paper documents containing PHI, it should be treated with the appropriate safeguards as a document removed from the University. Workforce Members must have approval prior to developing paper documents containing PHI while off premises and must document an inventory of the developed documents.

The security and return of the paper documents developed off premises are the sole responsibility of the Workforce Member who developed them. Documents containing PHI that are developed off the University premises must not be left unattended where 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.

2. Escorting Visitors, Vendors, and Patients. To ensure they do not have unauthorized access to PHI, during business hours, visitors, Vendors, 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, monitored, or governed by appropriate contracts, as applicable, based on the premises and the PHI stored on the premises. Vendors who are provided badge access to University premises should regularly be audited to ensure access is appropriate.

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 where patients are being seen or where PHI is located, without appropriate supervision.

3. Computers/Portable Computing Devices/Medical Devices ("Workstations"). Computer monitors must be protected from view, positioned away from common areas, or covered by a privacy screen to prevent unauthorized observation of PHI. Screens on Workstations must be returned to a password-protected screen saver or login screen when the Workstation will be unattended, even for short periods. If PHI must be stored on the actual Workstation (rather than on a secure server, as recommended), the Workstation must be encrypted.

Employees, volunteers, and trainees must use extreme caution when using Workstations to store PHI. PHI should not be stored on Workstations unless absolutely necessary; it should be stored on servers in a secure enterprise data center. If PHI is stored on Workstations including micro-desktops, the Workstation must be encrypted pursuant to HIPAA *Technical Safeguards* policy and applicable IT policies. Portable Computing Devices must never be left unattended in unsecured places. All micro-desktops that store PHI must be encrypted due to their portable nature.

Volunteers, except for volunteer faculty, are not authorized to store University 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.

4. Equipment. Equipment containing PHI (e.g., copiers, fax machines, scanners) 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. (See HIPAA *Tracking, Returning, and Disposing of Device and Media* policy.) The security and return of the equipment are the sole responsibility of the person who removes the equipment, as described in Section II. B (1)(b) above. The removal must be consistent with applicable University and Health Care Component procedure, 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 *Tracking, Returning, and Disposing of Device and Media* policy.

C. Theft or Loss. The theft or loss of any document, electronic medical record, or device containing Protected Health Information (including those owned by an individual) or of keys, or access cards to areas containing PHI shall be reported **immediately** to the University Privacy Official and/or HIPAA Security Officer, as appropriate, and to any person designated by the Health Care Component so that mitigation and reporting options can be considered and implemented as soon as possible. (See HIPAA *Breach of Unsecured PHI/ePHI* policy). The Information Technology *Loss of Computing or Storage Device Impact Assessment* form must be completed and submitted to IT Security (IT-Security@ouhsc.edu) for lost devices. Report to Local Law Enforcement is expected in case of theft of devices, keys, or access cards.

III. REFERENCES

A. HIPAA Privacy Regulations, 45 CFR 164.530
B. OUHSC Property Inventory § 581 (B)(2) and Equipment Inventory Off-Campus Usage Authorization Form, each as revised
C. Norman Campus Property Control, Temporary Equipment Use Agreement, as revised
D. HIPAA Security Regulations, 45 CFR 164.312 (a) – (b)