UNIVERSITY OF OKLAHOMA

HIPAA Policies

Title: Minimum Necessary Access and Rule	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Last Revised:** 4/1/18, 2/15/19, 7/22/22

I. PURPOSE

To describe the application of the Minimum Necessary Rule to Uses and Disclosures of and requests for Protected Health Information, including ePHI, by Workforce Members. The Minimum Necessary Rule provides that Uses and Disclosures of and requests for PHI must be limited to the least amount needed for this intended purpose.

II. POLICY*

A. The Minimum Necessary Rule provides that Workforce Members must make reasonable efforts to limit the Use and Disclosure of and requests for Protected Health Information to the minimum that is reasonably necessary for the Workforce Member to do his or her job, including to accomplish the intended purpose of the Use, Disclosure, or request.

The Minimum Necessary Rule does not apply to:

a. Disclosures to or requests by a Health Care Provider for Treatment purposes (excluding mental health and Substance Use Disorder Records);
b. Disclosures to the patient or his/her legal representative (See HIPAA *Personal Representatives* policy; and HIPAA *Patient Access to Own Protected Health Information* policy);
c. Uses or Disclosures made pursuant a Request for Health Information or an Authorization (See HIPAA *Authorization to Use or Disclose - Other Than to Patient PHI* policy);
d. Disclosures made to the Secretary of the Department of Health and Human Services for compliance and enforcement of the Privacy Regulations (See HIPAA *Required and Permitted Uses and Disclosures* policy);
e. Uses and Disclosures Required by Law (See HIPAA *Disclosures Required by Law* policy);
f. Uses and Disclosures required for compliance with HIPAA standardized transactions.

<u>Request for an Entire Medical Record</u>: Except as provided above, Workforce Members may not Use, Disclose, or request an entire medical record, except when the individual requesting the entire medical record specifically states in writing that the entire record is reasonably necessary to accomplish the purpose for the Use, Disclosure, or request.

Language such as the following should accompany requests for entire medical records:

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.

Based on my professional judgement, this request for the entire medical record is consistent with the Minimum Necessary Rule for the (describe) purpose intended.

B. Before access to PHI or ePHI can be established for a Workforce Member, the Health Care Component manager or administrator must authorize the User for the level of access appropriate for the User's responsibilities, as described below.

Each Health Care Component will implement and document a process for granting, reviewing, modifying, and terminating access to ePHI.

III. PROCEDURE FOR AUTHORIZING APPROPRIATE LEVEL OF ACCESS TO PHI

A. Access Authorization – Non-electronic PHI: Using the Role-Based Access Worksheet (available on the HIPAA website and from the Human Resources office), the manager or administrator (or his/her designee) of each HCC must document in writing:

1. The appropriate level of access to non-electronic PHI for each employee and volunteer. This must occur upon employment/appointment and when access requirements change.

2. The appropriate level of access to non-electronic PHI for the HCC's students and trainees, based on the educational activity and program. A student's or trainee's access would generally be determined and monitored as appropriate by the instructor/supervising individual.

B. Access Authorization – Electronic PHI: Using a document that the HCC manager or administrator or designee develops for each electronic system that maintains ePHI within the HCC (sample available from the HIPAA Security Officer), the manager or administrator of each HCC or his/her designee must determine and designate in writing:

1. The appropriate level of access to ePHI for each employee and volunteer. This must occur upon employment/appointment and when access requirements change.

2. The appropriate level of access to ePHI for the HCC's students and trainees, based on the educational activity and program. A student's or trainee's access would generally be determined and monitored as appropriate by the instructor/supervising individual.

For purposes of this policy, electronic systems include but are not limited to EMR systems; billing systems; and medical devices and equipment that store ePHI, such as ultrasound machines and medical monitors.

The HIPAA Security Officer, in consultation with the HCC administrator and IT Security, will assist in resolving any conflicts or discrepancies regarding the level of access to ePHI requested.

C. Access to PHI – Treatment Relationship: Workforce Members who are directly involved in a patient's Treatment (e.g., physicians and nurses) may have access to all of the patient's Protected Health Information, excluding mental health and Substance Use Disorder Records – access to these records is limited to the Minimum Necessary. Workforce Members who are not directly involved in a patient's Treatment should generally not have approved unlimited access to a patient's Protected Health Information -- access by these individuals is governed by the Minimum Necessary Rule.

D. Access to PHI – No Treatment Relationship: It is a violation of the Minimum Necessary Rule for a Health Care Provider to access the Protected Health Information of patients with whom the Provider has no Treatment relationship, unless for approved Research purposes, to perform a job responsibility, or as permitted by the HIPAA *Required and Permitted Uses and Disclosures* policy.

Family Member Records: Accessing records of a family member that are maintained in the University's electronic or paper system is a violation of the Minimum Necessary Rule unless the access is necessary for the performance of an assigned job duty.

Own Records: Employees may not access their own records that are maintained in the University's electronic or paper system. Employees who need access to or copies of their own records must submit the Request for PHI HIPAA form to the appropriate records office.

E. Access Documentation: Once access to ePHI has been authorized, the HCC manager, administrator, or designee will keep the documentation regarding approved access on file for a minimum of six years from the time access is terminated. Documentation for volunteers must be maintained by the HCC that is utilizing the volunteer, also for six years.

1. Each HCC shall designate an individual to notify Information Technology (and other offices that control access to systems containing ePHI such as the key shop, EMR department) when a User's employment or term of engagement has terminated or when the User's level of access to ePHI is no longer required. This notice may be via email or another expedient method, but it must be in writing and should generally occur on or before the day the access needs change.

2. Requests by any Workforce Member for access to disabled user accounts that may contain PHI must be made to the Office of Legal Counsel, who may consult with the University Privacy Official.

3. Reviews of documentation of User access levels will be conducted during the HIPAA compliance audits of each HCC. HCC managers and administrators should also verify periodically, such as during performance evaluations, that documented User access is appropriate and current.

IV. PROCEDURE FOR DISCLOSING PHI

A. Routine Disclosures: Routine Disclosures of PHI include responding to patient requests for medical records, subpoenas for records, and requests from attorneys for PHI. They occur on a routine or recurring basis. Each HCC manger or administrator shall have procedures documented for responding to routine requests for PHI.

B. Non-Routine Disclosures: Non-routine Disclosures of PHI (those that do not occur on a day-to-day basis as part of Treatment, Payment, or Health Care Operation activities or that are not Required by Law on a regular basis) shall not be made without first contacting the Office of Legal Counsel or the University Privacy Official. Examples include requests for PHI from state of federal agencies, search warrants, and media inquiries. The Office of Legal Counsel or University Privacy Official will give consideration to the following criteria: (a) the purpose of the request; (b) any potential harm that would result to the patient, the University, or any other third party as a result of the Disclosure; (c) the relevance of the information requested; and (d) other applicable state and federal laws and regulations.

When Disclosing PHI, Workforce Members may assume, if reasonable under the circumstances, that a request is for the minimum amount needed for the stated purpose when:

(a) making Disclosures to public officials as Required by Law, if the public official represents that the information requested is the minimum necessary for the stated purpose;

(b) the information is requested by another Covered Entity;

(c) the information is requested by a professional who is an employee of the University or is a Business Associate of the University providing professional services (if the request is for the entire medical record, the employee or Business Associate represents in writing that the information requested is the minimum necessary for the stated purpose); and

(d) documentation submitted by a researcher that the information is preparatory to Research or related to Research on a decedent or that the Disclosure has been approved by the IRB or Privacy Board.

V. PROCEDURE FOR MAKING REQUESTS FOR PHI

A. Routine Requests: Health Care Component managers and administrators must have standard procedures to limit the Protected Health Information their Workforce Members request on a routine or recurring basis to the minimum necessary for the intended purpose. Copies of the procedures shall be distributed within and maintained by each Health Care Component and provided to the Privacy Official upon request.

B. Non-Routine Requests: Health Care Component managers and administrators must designate an individual who will be responsible for reviewing all non-routine requests (those that do not occur on a day-to-day basis as part of Treatment, Payment or Health

Care Operation activities) for PHI. Any questions regarding the propriety or legality of a particular request must be submitted to the Office of Legal Counsel or the University Privacy Official, who will consider the following criteria: (a) the reason for the request; (b) any potential harm that would result to the patient, the University, or any other third party as a result of the Disclosure; (c) the relevancy of the information requested; and (d) other applicable state and federal laws and regulations.

VI. REFERENCES

A. HIPAA Privacy Regulations, 45 CFR 164.502(b)
B. HIPAA Privacy Regulations, 45 CFR 164.514(d)
C. HIPAA Security Regulations, 45 CFR 164.308(a)(4)