UNIVERSITY OF OKLAHOMA

HIPAA Privacy Policies

Subject: Introduction	**Page:** 1 of 1
Policy #: Privacy-00	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Last Revised:** January 27, 2016

I. POLICY*

It shall be the policy of the University[1] to protect and safeguard the Protected Health Information created, acquired, and maintained by its Health Care Components in accordance with the Privacy Regulations promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and as amended, and applicable state laws.

The Policies are intended to provide guidance to University Personnel in regard to the protection and enhancement of the privacy rights of patients by (a) establishing rules related to the internal and external Use and Disclosure of Protected Health Information; (b) affording patients access and information regarding the Use and Disclosure of their Protected Health Information; and (c) implementing administrative procedures intended to assist patients and University Personnel with regard to HIPAA.

These Policies apply to all Protected Health Information collected by Health Care Components after April 14, 2003. Policies governing the University's Health Plans are maintained on the Office for Human Resources and the HIPAA web pages.

These Policies supercede and replace any existing conflicting policies and procedures of any University Health Care Component relating to the Use and Disclosure and protection of Protected Health Information. Health Care Components may maintain additional policies and procedures relating to the Use and Disclosure and protection of Protected Health Information only to the extent that they do not conflict with these Policies. Health Care Components may add to or supplement the Policies or the related forms, but they may not delete or revise any without first consulting the University Privacy Official.

These Policies apply to all Protected Health Information, regardless of the form in which it is created or maintained (oral, written, or electronic).

These Policies apply to the Protected Health Information of both living and deceased patients.

[1] The University is a Hybrid Entity with designated Health Care Components. See, Privacy-01,Definitions.

*Capitalized terms are defined in Privacy-01, Definitions

UNIVERSITY OF OKLAHOMA

HIPAA Privacy Policies

Subject: Definitions	**Page:** 1 of 7
Policy #: Privacy-01 (Definitions)	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Last Revised:** January 27, 2016

I. DEFINITIONS

A. Unless otherwise provided, the definitions below apply to all of the University's Privacy and Security Policies. These terms are capitalized when used in the Policies to indicate that they have been uniquely defined by the University or federal law.

1. Authorization. The formal grant of authority by a patient to a Covered Entity or Health Care Component to Use or Disclose the patient's Protected Health Information. 45 C.F.R. § 164.508 (c).

~~1.~~2. Breach. The acquisition, access, Use or Disclosure of Protected Health Information in a manner not permitted under the Privacy Regulations that compromises the security or privacy of the Protected Health Information. 45 C.F.R. § 164.402.

~~2~~3. Business Associate. A person or entity not employed by the University that creates, receives, maintains, or transmits Protected Health Information for a covered function or activity, for or on behalf of the University. Such activities may include, but are not limited to, billing; repricing; claims processing and administration; data analysis; legal, accounting, and actuarial services; certain patient safety activities; consulting; utilization review; quality assurance; and similar services or functions. A Business Associate may be a Covered Entity. 45 C.F.R. § 160.103.

~~3~~4. Compliance Date. The date by which a Covered Entity must comply with the Privacy Regulations, which is April 14, 2003.

~~4~~5. Correctional Institution. Any penal or correctional facility, jail, reformatory, detention center, work farm, halfway house, or residential community program center operated by, or under contract to, the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe for the confinement or rehabilitation of persons charged with or convicted of a criminal offense or other persons held in lawful custody. Other persons held in lawful custody include juvenile offenders, adjudicated delinquent aliens detained awaiting deportation, persons committed to mental institutions through the criminal justice system, witnesses, or others awaiting charges or trial. 45 C.F.R. § 164.501.

~~5~~6. Covered Entity. The entities to which the Privacy Regulations apply, including the University because it is a Health Plan and/or a Health Care Provider that transmits any Health Information in electronic form in connection with one of the following eleven transactions: (i)

Health Care claims or equivalent encounter information; (ii) Health Care payment and remittance advice; (iii) coordination of benefits; (iv) Health Care claims status; (v) enrollment and disenrollment in a health plan; (vi) eligibility for a health plan; (vii) health plan premium payments; (viii) referral certification and authorization; (ix) first report of injury; (x) health claims attachments; and (xi) other transactions that the Secretary of DHHS may prescribe by regulation. 45 C.F.R. § 160.103.

~~6~~7. Covered Functions. Those functions of a Covered Entity, the performance of which makes the entity a Health Care Provider. 45 C.F.R. § 160.103.

~~7~~8. Designated Record Set. A group of records maintained, collected, Used, or disseminated by or for a University Health Care Component that includes the medical and billing records about individuals; or the enrollment, payment, claims adjudication, and case or medical management records systems; that is used, in whole or in part, by University Personnel to make decisions about individuals, regardless of who originally created the information. A Designated Record Set does not include: (a) duplicate information maintained in other systems; (b) data collected and maintained for Research; (c) data collected and maintained for peer review or risk management purposes; (d) Psychotherapy Notes; (g) information compiled in reasonable anticipation of litigation or administrative action; (h) employment records; (i) education records covered by FERPA; (j) information subject to 42 USC 263a (CLIA) or exempt under 42 CFR 493.3(a)(2) (CLIA); and (k) source data interpreted or summarized in the individual's medical record (example: pathology slide and diagnostic films). 45 C.F.R. § 164.501.

The definition of a Designated Record Set refers only to the official record for the patient and not to duplicate information maintained in other systems.

~~8~~9. Disclose or Disclosure. The release, transfer, provision of access to, or divulging in any other manner of information **outside** the University's Health Care Components.45 C.F.R. § 160.103. (See also, Use.)

Exchange of Protected Health Information with a department or area of the University that is not designated as a Health Care Component is considered a Disclosure, subject to HIPAA.

~~9~~10. Direct Treatment Relationship. A treatment relationship between an individual and a Health Care Provider that is not an Indirect Treatment Relationship. 45 C.F.R. § 164.501.

~~10~~11. Health Care. Care, services, or supplies related to the health of an individual. Health Care includes, but is not limited to, the following: (a) preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition or functional status of an individual or that affects the structure or function of the body; and (b) sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription. 45 C.F.R. § 160.103.

~~11~~12. Health Care Component(s). A component or combination of components designated by the University, a Hybrid Entity. The "Health Care Components" of the University of Oklahoma include the parts ~~or all~~ of the following that provide Covered Functions: (a) College of Medicine – Oklahoma City, including OU Physicians; (b) OU School of Community Medicine (formerly College of Medicine – Tulsa), ~~and~~ including OU Physicians-Tulsa; (c)

College of Pharmacy; (d) College of Dentistry; (e) College of Nursing; (f) College of Allied Health; (g) College of Public Health; (h) Development Office; (i) Goddard Health Center; (j) Athletics Department (Center for Athletic Medicine and Psychological Resources for OU Student-Athletes); (k) Information Technology; (l) Internal Auditing; (m) Office of Legal Counsel; (n) Counseling Psychology Clinic;* (o) HSC Financial Services; (p) NC Financial Support Services; (q) Office of Compliance; (r) Human Research Participant Protection Program/Institutional Review Board; and (s) HSC Student Counseling Services;* (t) University Printing Services; and (u) Waste Management – Norman Camus.

As "Health Care Component" is used in the University's Privacy Policies, it will include all of the constituent parts of a Health Care Component (e.g. departments and clinics) that perform covered functions and the University Personnel providing Health Care services on behalf of the Health Care Component, unless circumstances clearly indicate otherwise.

~~12~~13. Health Care Operations. "Health Care Operations" means any of the following activities of the University to the extent that the activities are related to Covered Functions:

(a) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing Health Care costs; protocol development; case management and care coordination contacting of University Personnel and patients with information about treatment alternatives; and related functions that do not include treatment;

(b) Reviewing the competence or qualifications of Health Care professionals; evaluating practitioner and provider performance and health plan performance; conducting training programs in which students, trainees, or practitioners in areas of Health Care learn under supervision to practice or improve their skills as University Personnel; training of non-Health Care professionals; accreditation, certification, licensing, or credentialing activities;

(c) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;

(d) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the University, including formulary development and administration, development, or improvement of methods of payment or coverage policies; and

(e) Business management and general administrative activities of the University, including, but not limited to: (1) management activities relating to implementation of and compliance with the University's Privacy Policies; (2) resolution of internal grievances; (3) due diligence related to the sale, transfer, merger, or consolidation of all or part of a Health Care Component with another Covered Entity; and (4) creating de-identified Health Information or a limited data set and fundraising for the benefit of a Health Care Component(s). 45 C.F.R. § 164.501.

* By policy only

~~13~~14. Health Care Provider. A provider of services (as defined in § 1861(u) of the Social Security Act, 42 U.S.C. § 1395x(u)), a provider of medical or health services (as defined in § 1861(s) of the Act, 42 U.S.C. § 1395x(s)), and any other person or organization who furnishes, bills, or is paid for Health Care in the normal course of business. 45 C.F.R. § 160.103.

~~14~~15. Health Information. Any information, whether oral or recorded in any form or medium, that: (a) is created or received by a Health Care Provider…employer…school or university… and (b) relates to the past, present, or future physical or mental health or condition of an individual; the provision of Health Care to an individual; or the past, present, or future payment for the provision of Health Care to an individual. 45 C.F.R. § 160.103.

~~15~~16. Health Oversight Agency. An agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the Health Care system (whether public or private) or government programs in which Health Information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which Health Information is relevant. 45 C.F.R. § 164.501.

~~16~~17. HIPAA. The Health Insurance Portability and Accountability Act of 1996.

~~17~~18. HITECH. The Health Information Technology for Economic and Clinical Health Act, passed on February 17, 2009.

~~18~~19. Hybrid Entity. A single legal entity: (1) that is a Covered Entity; (2) whose business activities include both Covered and non-Covered functions; and (3) that designates Health Care Components. 45 C.F.R. § 164.504. (The University is a Hybrid Entity. See also, Health Care Components.)

~~19~~20. Indirect Treatment Relationship. A relationship between an individual and a Health Care Provider in which: (a) the Health Care Provider delivers Health Care to the individual based on the orders of another Health Care Provider; and (b) the Health Care Provider typically provides services or products or reports the diagnosis or results associated with the Health Care directly to another Health Care Provider, who provides the services or products or reports to the individual. 45 C.F.R. § 164.501.

~~20~~21. Individually Identifiable Health Information. Information that is a subset of Health Information, including demographic information collected from an individual, and that (a) is created or received by a Health Care Provider, health plan, employer, or health care clearinghouse; and (b) relates to the past, present, or future physical or mental health or condition of an individual; the provision of Health Care to an individual; or the past, present, or future ~~payment~~ Payment for the provision of Health Care to an individual; and (i) that identifies the individual; or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual. 45 C.F.R. § 160.103

~~21~~22. Inmate. A person incarcerated in or otherwise confined to a Correctional Institution. 45 C.F.R. § 164.501.

~~22~~23. Law Enforcement Official. An officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe who is empowered by law to: (i) investigate or conduct an official inquiry into a potential violation of law; or (ii) prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law. 45 C.F.R. § 164.103.

~~23~~24. Legal Counsel. The University's Office of Legal Counsel and the attorneys and staff who work in or for the office.

~~24~~25. Marketing. ~~To make a communication about a product or service that encourages recipients of the communication to purchase or use the product or services unless the communication is made: (a) to describe a health-related product or service (or payment for such product or service) that is provided by the University, including communications about the entities participating in a Health Care Provider network or health plan network and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits; (b) for Treatment of the individual; or (c) for case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, Health Care Providers, or settings of care to the individual~~See, Privacy-28, Marketing.~~.~~

~~25~~26. Organized Health Care Arrangement. A clinically integrated care setting in which the individuals typically receive Health Care from more than one Health Care Provider (example: a hospital and members of its medical staff). 45 C.F.R. § 164.501.

~~26~~27. Particularly Sensitive Health Information. Protected Health Information that is generally considered highly confidential including, but not limited to, mental health, drug and alcohol abuse, and communicable disease information.

~~27~~28. Payment. Any activities by the University or a Health Care Component to obtain payment for providing Health Care. Such activities relate to the individual to whom Health Care is provided and include, but are not limited to: (a) billing, claims management, collection activities, and related Health Care data processing; and (b) Disclosure to consumer reporting agencies of any of the following Protected Health Information relating to collection of premiums or reimbursement: (i) name and address; (ii) date of birth; (iii) Social Security number; (iv) payment history; (v) account number; and (vi) name and address of the Health Care Provider. 45 C.F.R. §164.501.

~~28~~29. Personal Representative. ~~See~~ Privacy ~~Policy~~-02, ~~"~~Personal Representatives.~~"~~

~~29~~30. Protected Health Information or PHI. Individually Identifiable Health Information that is transmitted by, or maintained in, electronic media or any other form or medium. 45 C.F.R. §160.103.

Protected Health Information excludes Individually Identifiable Health Information ~~in~~: (a) in education records covered by the Family Educational Rights and Privacy Act (FERPA); ~~and~~ (b) in employment records held by the University in its role as employer; and (c) regarding an individual who has been deceased more than 50 years.

~~30~~31. Privacy Policies or Policies. This set of policies drafted and adopted by the University ~~for the use of its Health Care Components~~ relating to the protection and confidentiality of Protected Health Information.

~~31~~32. Privacy Regulations. The regulations issued by the Department of Health and Human Services implementing the privacy requirements of the Health Insurance Portability Act of 1996 (HIPAA), 42 CFR Parts 160 and 164, aimed at protecting a patient's right to privacy in matters involving his or her Health Care, as may be amended.

~~32~~33. Psychotherapy Notes. Notes recorded in any medium by a Health Care Provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record.

> ***Psychotherapy Notes*** **exclude medication prescription and monitoring, counseling session~~s~~ start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, ~~the~~ treatment plan, symptoms, prognosis, and progress to date. 45 C.F.R § 164.501.**

~~33~~34. Public Health Authority. An agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate. 45 C.F.R. § 164.501.

~~34~~35. Required by Law. A mandate contained in law that compels the University to make a Use or Disclosure of Protected Health Information and that is enforceable in a court of law. Required by Law includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summonses issued by a court, grand jury, governmental or tribal inspector general, or administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to Health Care Providers participating in the program; and statutes or regulations that require the production of information, including those that require such information if payment is sought under a government program providing public benefits. 45 C.F.R. § 164.501.

~~35~~36. Research. A systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge. 45 C.F.R § 164.501.

~~36~~37. Treatment. The provision, coordination, or management of Health Care and related services ~~by University Personnel~~. 45 C.F.R. § 164.501.

> **Treatment includes: (a) the coordination or management of Health Care by a Health Care Provider with a third party; (b) consultation between Health Care Providers relating to a patient; or (c) the referral of a patient for Health Care from one Health Care Provider to another. 45 C.F.R. § 164.501.**

~~37~~38. University. The University of Oklahoma, including its officers, employees, and agents when the context clearly intends such.

~~38~~39. University Personnel. Faculty, staff, volunteers, students and other trainees, and other persons whose conduct, in the performance of work for the University or its Business Associates, is under the direct control of the University or its Business Associate, whether or not they are paid by the University or its Business Associate ("~~w~~Workforce Members"). 45 C.F.R. § 160.103.

~~39~~40. Use. With respect to Individually Identifiable Health Information, the sharing, employment, application, utilization, examination, or analysis of such information **within** the University by Health Care Components. 45 C.F.R. § 164.501. (See also, Disclosure.)

~~40~~41. Workforce Member. See University Personnel.

II. REFERENCES

A. 45 C.F.R. 160.103
B. 45 C.F.R. 164.501

UNIVERSITY OF OKLAHOMA

HIPAA Privacy Policies

Subject: Personal Representative	**Page:** 1 of 4
Policy #: Privacy-02 (Uses & Disclosures)	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Last Revised:** January 19, 2016

I. PURPOSE

To establish who can act on behalf of the patient for purposes of Authorizing Uses and Disclosures and exercising the patient rights provided by these Policies.

II. POLICY*

A Health Care Component must, except in the limited circumstances ~~set forth~~ explained in this Policy, treat a Personal Representative as if he were the patient for purposes of determining who may authorize ~~Authorizing~~ Uses and Disclosures and ~~exercising~~ exercise the patient rights provided by these Policies. *However, the Personal Representative must be treated as the individual patient only to the extent that the Protected Health Information is relevant to matters on which the Personal Representative is Authorized to represent the patient.*

If University Personnel have a reasonable belief that the Personal Representative has abused or neglected the patient or that treating the Personal Representative as the patient could endanger the patient~~,~~ and believe it is not in the patient's best interest to treat the person as the patient's Personal Representative, University Personnel are not required to treat the Personal Representative as the patient. See, Privacy-05, Patient Access to Protected Health Information.

A. Personal Representatives for Adults

Adults can act as a Personal Representative of another adult if they possess documentation of the following:

1. Durable Power of Attorney for Health Care. A durable power of attorney is a document by which the patient may designate an individual as his~~/her~~ agent to perform certain acts on his~~/her~~ behalf. Under a valid durable power of attorney, and *depending on the scope of the power of attorney*, the agent may make health and medical care decisions on the patient's behalf. Note: A Durable Power of Attorney ~~This~~ does not give the agent the power to execute an advance directive for health care, living will, or other document to authorize life-sustaining treatment decisions or to make life-sustaining treatment decisions unless the power of attorney complies with the requirements for a Health Care Proxy.

A valid Durable Power of Attorney must be in writing and contain the words "*This power of attorney shall not be affected by subsequent disability or incapacity of the principal, or lapse of time*," or "*This power of attorney shall become effective upon disability or incapacity of the*

principal," or similar words showing the intent of the patientprincipal that the power of attorney authority conferred will be exercisable notwithstanding the principal's (even in cases of the patient's) subsequent disability or incapacity. The document should must state whether University Personnel may rely on the power of attorney while the patient is still competent or whether it the power is effective when the patient is competent or only once the patient becomes incompetent.

The patient may revoke the power of attorney at any time if competent. Death of the patient also will revoke and terminate the power of attorney. The execution of a Durable Power of Attorney should must be witnessed by two witnesses who are at least 18 years old. The signatures of the patient and witnesses should must be notarized.

2. Health Care Proxy. A Health Care Proxy is an adult appointed by a patient to make health care decisions, including but not limited to withholding or withdrawing of life-sustaining treatment, in certain circumstances pursuant todescribed in an advanced directive for health care decision. A Health Care Proxy's authority becomes effective only (a) when the patient is incompetent and (b) has been diagnosed with a terminal condition or as persistently unconscious. The directive must be in writing, signed by the patient, and witnessed by two disinterested witnesses. (A disinterested witness is a witness who is at least 18 years old and who does not have an interest in the patient's estate.)

The appointment of the Health Care Proxy may be completely or partially revoked at any time and in any manner by the patient. A revocation is effective upon when the patient communicatesion of the desire to revoke to the attending physician or other University Personnel. If the patient revokes the advanced directive, a the Health Care Proxy may no longer qualifiesy as a Personal Representative.

3. Court-Appointed Guardian. This is a person appointed by the court in a court order who legally has authority over the care and management of the person, estate, or both, of a patient who cannot act for him/herself. This order may place certain limitations on the legal activities of the guardian.

4. Individuals Designated in Experimental Treatment Statute. The Oklahoma Experimental Treatment statute, 63 Okla. Stat. 3102A, provides that a legal guardian, attorney-in-fact, and certain enumerated family members may consent to an incapacitated adult patient's participation in a research study being conducted by a University faculty member who has received IRB approval for the study.

B. Personal Representatives for Minors

1. Medical Treatment. For a minor patients (under the age of 18) who does not fall within one of the exceptions listed below, either parent, the legal guardian, or the legal custodian appointed by a court may act as a the minor's Personal Representative.

A minor may act on his/her own behalf in making treatment decisions in the following instances:

a. Any minor who is married, has a dependent child, or is emancipated.

b. Any minor who is separated from his/her parents or legal guardian and is not supported by them.

c. Any minor who is or has been pregnant or afflicted with any reportable communicable disease, drug and substance abuse, or abusive use of alcohol, but only if the minor is seeking treatment, diagnosis, or prevention services related to such conditions. If the minor is found not to be pregnant or suffering from a communicable disease, drug or substance abuse, or abusive use of alcohol, University Personnel shall not reveal any information to the spouse, parent, or Personal Representative of the minor without the minor's consent.

d. Any minor as to his/her minor child.

e. The spouse of a minor if the minor is incapable of consenting because of physical or mental incapacity.

f. Any minor who by reason of physical or mental capacity cannot give consent and has no known relatives or legal guardian, if two physicians agree on the health service to be given.

g. Any minor in need of emergency services for conditions that will endanger his health or life if delay would result by obtaining consent from his spouse, parent, or legal guardian; provided, however, that the prescribing of any medicine or device for the prevention of pregnancy shall not be considered such an emergency service.

Note: If any minor falsely represents that he may give consent and a health professional provides health services in good faith based upon that misrepresentation, the minor shall receive full services without the consent of the minor's parent or legal guardian and the health professional shall incur no liability except for negligence or intentional harm. Consent of the minor shall not be subject to later disaffirmance or revocation because of his minority.

Except as set forth in paragraph c above, University Personnel are required to make a reasonable attempt to inform the spouse, parent, or guardian of the minor of any emergency services provided to the categories of minors set forth above. In all other instances, University Personnel may, but are not required to, inform the spouse, parent, or legal guardian of the minor of any treatment provided.

2. Experimental Procedures/Treatment. Information regarding who may consent for minors to participate in Research and under what circumstances may be obtained from the University's ~~IRB~~ HRPP Office or Office of Legal Counsel.

C. Personal Representatives for Deceased Individuals

If under applicable law, there is an executor, administrator, or other person having authority to act on behalf of a deceased individual or of the individual's estate, that individual must be treated as the Personal Representative of the deceased, with respect to PHI, and may

Authorize the Use or Disclosure of the deceased patient's Personal Health Information. The court document appointing the individual as an executor or administrator is known as the Letters Testamentary or Letters of Administration and ~~should be~~is signed by a judge. Under Oklahoma law, the following individuals have authority to act as a Personal Representative if there is no executor or administrator appointed: the spouse of the deceased or, if no spouse, any responsible family member of the deceased. A responsible family member is a parent, adult child, adult sibling, or other adult relative of the deceased who was actively involved in providing or monitoring the care of the deceased, as verified by the doctor, hospital, or other medical institute that was responsible for providing care and treatment of the deceased.

The University must comply with HIPAA with respect to the Protected Health Information of deceased individuals for a period of 50 years following the death of the individual.

III. PROCEDURES

A. University Personnel must review a copy of the document conferring Personal Representative status to ensure the Personal Representative's authority is not limited in scope or time and to ensure it meets the requirements described above. Any questions regarding the validity of a document purporting to confer Personal Representative status must be directed to the Office of Legal Counsel.

B. University Personnel must verify the identity of the individual requesting Protected Health Information if the individual is not known. (See, Privacy-03, Verification of Identity Policy.)

C. A copy of the written document appointing a person as the Personal Representative of a patient should be placed in the patient's medical record as verification of the individual's authority.

IV. REFERENCES

A. 58 Okla. Stat. 1072.1
B. 63 Okla. Stat. 3101.1
C. 63 Okla. Stat. 3102A
D. 63 Okla. Stat. 2602; 76 O.S. 19
E. 45 C.F.R. 164.502 (g)

UNIVERSITY OF OKLAHOMA

HIPAA Privacy Policies

Subject: Verification of Identity	**Page:** 1 of 2
Policy #: Privacy-03 (Uses & Disclosures)	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Last Revised:** January 27, 2016

I. PURPOSE

To establish an identity verification process to be used when Disclosing PHI. ~~(This process is not required for Disclosure to family members or others involved in the patient's care, pursuant to Privacy-26, Uses and Disclosures to Family and Others Involved in Patient's Care.)~~

II. POLICY*

A. Prior to making a Disclosure or processing a patient request permitted by these Policies, unless otherwise stated in ~~the~~ this Policy, University Personnel must: (i) verify the identity of a person requesting Protected Health Information and the authority of any such person to have access to Protected Health Information, if the identity or any such authority of such person is not known to University Personnel; and (ii) obtain and copy any documentation, statements, or representations, whether oral or written, from the person requesting the Protected Health Information when such documentation, statement, or representation is a condition of the Disclosure or processing.

~~A.~~B. This process is not required for Disclosure to family members or others involved in the patient's care, pursuant to Privacy-26, Uses and Disclosures to Family and Others Involved in Patient's Care.

~~B.~~C. Subject to Section III below, to verify identity, University Personnel may rely on:

1. An administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law provided that the information sought is relevant and material to a legitimate Law Enforcement inquiry, the request is specific and limited in scope, and de-identified information could not reasonably be used. (See Privacy-25, Required by Law, Section D (2).)

2. Appropriately executed documentation of an IRB or Privacy Board waiver or alteration of the Authorization requirement.

3. A request by an authorized public official upon presentation of his/her badge or other official credentials if in person or the appropriate letterhead if the request is made in writing. Authority may be verified by written statement or legal process, warrant, subpoena, order, or other legal process. (This goes to verification of identity of the

*Capitalized terms are defined in Privacy-01, Definitions

official only; to determine whether the official is entitled to obtain the Protected Health Information, See Privacy-25, Required by Law; and Privacy-20, Uses and Disclosures; or contact the Office of Legal Counsel or the University Privacy Official.)

4. Personal judgment if a Disclosure is being made solely to avert a serious threat to health or safety or in cases when a patient is required to be given an opportunity to agree or object to the Disclosure.

Verification of identity can be accomplished by: (1) review of picture I.D.; (2) signature comparison; or (3) other appropriate method. Determination of whether the individual is authorized to obtain PHI is still required. See Privacy-20, Uses and Disclosures — General and Privacy-26, Disclosures to Family and Others Involved in Patient Care.

III. PROCEDURES

Any questions regarding verification of or reliance on identity or authority should be directed to the ~~Supervisor~~supervisor, the Office of Legal Counsel, or the University Privacy Official. The Office of Legal Counsel or the University Privacy Official should be contacted prior to responding to any request by Law Enforcement Officials.

IV. REFERENCES

A. Privacy-20, Uses and Disclosures, and Privacy-25, Required by Law
B. 45 C.F.R. §164.514 (h) (1)

UNIVERSITY OF OKLAHOMA

HIPAA Privacy Policies

Subject: Notice of Privacy Practices	**Page:** 1 of 3
Policy #: Privacy-04 (Patient Rights)	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Last Revised:** January 27, 2016

I. PURPOSE

To require the development and distribution of a Notice of Privacy Practices.

II. POLICY*

The University, through the Privacy Official, will develop and distribute a Notice of Privacy Practices for its Health Care Components that includes the information required by the Privacy Regulations. A patient's receipt of the Notice of Privacy Practices must be acknowledged as required by the Privacy Regulations. (See Acknowledgement of Receipt of Notice of Privacy Practices form.)

The Notice of Privacy Practices shall be available in Spanish. Each HCC shall have the Notice translated into other languages based on its patient population and as required by regulations issued by the Office for Civil Rights regarding accommodations for people with Limited English Proficiency.

University Personnel may not use or disclose Protected Health Information in a manner inconsistent with the University's Notice of Privacy Practices.

III. PROCEDURE

A. Acknowledgement of Receipt of Notice of Privacy Practices

A Notice of Privacy Practices must be provided to each patient at the first appointment for services within a Health Care Component. The patient will be asked to sign the Acknowledgment of Receipt of Notice of Privacy Practices at this time. If the patient does not acknowledge receipt of the Notice of Privacy Practices, a note ~~should~~ shall be made on the registration form or in the patient's medical record indicating why the acknowledgement was not obtained. Health Care Components ~~should~~ may not condition Treatment on the patient's signature Acknowledgement of Receipt of the Notice of Privacy Practices.

The preferred method for obtaining acknowledgement is to require the patient sign the Acknowledgement of Privacy Practices form.

B. Distribution of Notice of Privacy Practices

1. University Health Care Components must make the Notice of Privacy Practices

available to any person who requests it. The individual making the request does not have to be a patient of the University.

2. Health Care Components must ensure that Health Care Providers with Direct Treatment relationships with patients:

a. Provide the Notice of Privacy Practices to each patient no later than the date of the first service delivery~~, including service delivered electronically~~. If the first service delivery to an individual is delivered electronically, the Health Care Component ~~patient~~ must ~~be~~ provide the patient with an electronic copy of the Notice of Privacy Practices and the Acknowledgment of Receipt of the Notice automatically and contemporaneously in response to the individual's first request for service. If the first service delivery is via telephone, the Notice and Acknowledgment of Receipt of Notice must be mailed the same day of service.

During emergency treatment situations, the Notice of Privacy Practices may be provided and the Acknowledgement obtained as soon as reasonably practicable after the emergency is resolved.

b. Make the Notice of Privacy Practices available at the service delivery site upon request.

c. Post the Notice of Privacy Practices in a clear and prominent location where it is reasonable to expect individuals seeking service from the Health Care Provider to be able to read it.

3. The Notice may be distributed by e-mail if the patient agrees to the electronic notice and the agreement has not been withdrawn. (See Electronic NPP form.) All timing requirements for distribution of the NPP also apply to electronic notices. If University Personnel know that the electronic transmission has failed, a hard copy must be provided. When electronic notice is provided, an Acknowledgement of Receipt of NPP still must be ~~obtained~~provided to the patient for return.

4. Health Care Components ~~must require that Health Care Providers~~ with **Indirect** Treatment Relationships with patients must provide the Notice of Privacy Practices to individuals upon request.

5. The Notice of Privacy Practices or a link to the Notice on the HIPAA web page ~~for the Health Care Components~~ must be posted on the web sites of the Health Sciences Center (both Oklahoma City and Tulsa campuses), the Norman campus, Goddard Health Center, and the Office of Compliance. Any College, department, or clinic that maintains its own web site also must post the Notice of Privacy Practices on its web site or include a link to the Notice on the HIPAA webpage.

C. Amendment ~~of~~ Notice of Privacy Practices

If the Notice of Privacy Practices is amended, the amended version must be posted and

distributed to new patients. It also must be made available upon request to current patients. (See also Privacy-15, Development and Amendment of Privacy Policies and Procedures.)

D. Retention

The Notice of Privacy Practices must be retained by the Privacy Official for six years.

IV. REFERENCES

A. HIPAA Privacy Regulations, 45 C.F.R. 164.520

UNIVERSITY OF OKLAHOMA

HIPAA Privacy Policies

Subject: Patient Access to Protected Health Information	**Page:** 1 of 5
Policy #: Privacy-05 (Patient Rights)	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Last Revised:** January 27, 2016

I. PURPOSE

To address issues related to patient access to their Protected Health Information maintained in a Designated Record Set.

II. POLICY*

A. Rights to Access

The University will permit patients to inspect and obtain a copy of their Protected Health Information that is included in a Designated Record Set and maintained by a Health Care Component, for as long as the Protected Health Information is maintained in the Designated Record Set. If the same information is kept in more than one Designated Record Set or in more than one location, the University has to produce the information only once per request for access. The patient ~~should~~ must complete an Authorization for Use or Disclosure of Protected Health Information, as required in Privacy-23, Authorization.

Unless an exception applies, a patients ~~should~~ shall be granted access to ~~the entire medical record~~their PHI maintained in a Designated Record Set, including records received from other providers ~~that were~~ used to make Treatment decisions.

The University may charge a fee for access to Protected Health Information as long as the fee is consistent with any limit set by state and federal law. Current charges are available on the HIPAA webpage and/or HIPAA and Authorization forms.

The University must provide the patient with access to the Protected Health Information in the form or format requested by the patient, if it is readily producible in such form or format; or, if not, in a readable hard copy form or other form or format as agreed to by the University and the patient. If the Protected Health Information is maintained in an electronic health record, the University must provide the patient with a copy of the Protected Health Information in electronic format, upon request.

The University must arrange with the patient for a convenient time and place to inspect or obtain a copy of the Protected Health Information or mail or fax a copy of the information at the patient's request. (See Privacy-18, Safeguards for information on emailing PHI.)A Health Care Component may discuss the scope, format, and other aspects of the request for access with the

patient as necessary to facilitate the timely provision of access.

If the University does not maintain the Protected Health Information that is the subject of the patient's request for access and University Personnel know where the requested information is maintained, the University must inform the patient where to direct the request for access.

B. Psychotherapy Notes

A patient does not have the right to access Psychotherapy Notes relating to him/herself except (i) to the extent the patient's treating professional approves such access in writing; or (ii) the patient obtains a court order authorizing such access. (See Psychotherapy Notes, Privacy-01, Definitions; and Privacy-24, Mental Health.)

C. Denial of Right to Access

A patient may be denied access to Protected Health Information under the limited circumstances listed below. **The following exceptions should be narrowly construed and rarely used:**

1. Legal Information. The University may deny a patient access to information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding. The advice of the Office of Legal Counsel or the Privacy Official should be obtained prior to denying a patient's request for access on this basis.

2. Inmate Information. The University, acting under the direction of a Correctional Institution, may deny, in whole or in part, an inmate's request to obtain a copy of Protected Health Information, if obtaining it would jeopardize the health, safety, security, custody, or rehabilitation of the patient or of other inmates, or the safety of any officer, employee, or other person at the Correctional Institution or entity responsible for transporting the inmate.

3. Research. The University may temporarily suspend a patient's access to Protected Health Information created or obtained in the course of Research that includes Treatment. The suspension may last for as long as the Research is in progress, provided that the patient has agreed to the ~~denial~~ suspension of access when consenting to participate in the Research and the patient has been informed that the right of access will be reinstated upon completion of the Research.

4. Information from Other Source. The University may deny a patient's access to Protected Health Information if the information was obtained from someone other than a Health Care Provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

5. Endangerment. The University may deny a patient access to Protected Health Information in the event a licensed Health Care Professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the patient or another person. Access may not be denied on the basis of the sensitivity of the Health Information or the potential for causing emotional or psychological

harm.

6. Reference to Other People. The University may deny a patient access to Protected Health Information if it makes reference to another person and a licensed Health Care Professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person. Access can be denied if the release of such information is reasonably likely to cause substantial physical, emotional, or psychological harm to the other person.

7. Personal Representative. The University may deny access to Protected Health Information if the request is made by a patient's Personal Representative and a licensed Health Care Professional has determined, in the exercise of professional judgment, that the provision of access to such Personal Representative is reasonably likely to cause substantial harm to the patient or another person. (See Privacy-02, Personal Representative.)

8. Psychotherapy Notes. See Paragraph B above.

9. CLIA Information. The University may deny access to PHI that is subject to 42 USC 263a if such access would be prohibited by law, or to PHI that is exempt under 42 CFR 493.3(a)(2), CLIA.

10. Privacy Act. The University may deny access to PHI that is in records subject to the Privacy Act, if denial meets the requirements of the Act. ~~Contact t~~The Office of Legal Counsel or the University Privacy Official should be contacted prior to denying access on this basis.

The University must, to the extent possible, give the patient access to any other Protected Health Information requested, after excluding the Protected Health Information to which access is being denied.

D. Review of Denied Access

If access to Protected Health Information is denied for the reasons set forth in Paragraph C 5, 6, or 7 above, the patient must be given the opportunity to have the denial reviewed by a licensed Health Care Professional in the clinic that received the request or some other appropriate person designated by the Health Care Component that maintains the records requested ("Reviewer"). The Reviewer cannot have participated in the original denial. The Denial of Individual's Request for PHI form, available on the HIPAA website, must be used to ensure this information is provided to the individual.

III. PROCEDURES

A. Rights to Access

1. All patients must make their requests for access in writing using the University's Authorization to Release/Request for an Individual's Health Information/Treatment and Education Records ~~Request for Individual's Health Information form~~ (Authorization form) or

another form that complies with HIPAA and ~~state~~ Oklahoma law. Patients making their request for access by telephone or e-mail ~~should~~ must be sent a copy of the Authorization form or referred to the University's HIPAA forms webpage. **Verification of the requester's identity must be obtained prior to granting access to the Protected Health Information.** (See Privacy-03, Verification of Identity.) The form must be maintained in the patient's medical record for a minimum of six (6) years.

2. If a patient indicates on the form that he/she has been treated by more than one Health Care Component, the Health Care Component that received the request ~~should~~ shall immediately forward a copy of the request to the University Privacy Official, who will coordinate the processing of the request with the other Health Care Components designated by the patient. If the patient does not request access from any other Health Care Components, the Health Care Component that received the initial request ~~should~~ shall process the request in accordance with its internal procedures and maintain a copy of the form in the patient's medical record. A copy of the Denial form, if applicable, ~~should~~ shall also be filed in the patient's medical record and, upon request, sent to the Privacy Official.

3. A patient's request for access to Protected Health Information must be acted upon as soon as reasonably possible, but in no event more than thirty (30) calendar days after the request is received~~receiving the request~~. No extensions are permitted without prior approval of the University Privacy Official, who may approve an additional 30 days in compliance with the law.

4. Each Health Care Component must designate and document the titles of persons or offices responsible for receiving and processing requests for access to Protected Health Information. A copy of the designations must be provided to the University Privacy Official upon request. The Health Care Components must update the list as changes are made and provide an updated list to the University Privacy Official, who will maintain a copy of the designations for a minimum of six (6) years.

5. Any questions regarding a patient's right of access should be forwarded to the University Privacy Official or the Office of Legal Counsel.

The Health Care Provider who treated the patient should be notified by the Health Care Component designee if a patient requests access to his/her Protected Health Information for litigation or some other unusual purpose.

B. Denial of Right to Access

If a patient's request for access to Protected Health Information is denied, the patient must be provided with a written denial using the University's Denial of Request for Protected Health Information form. The form must be maintained in the patient's medical record for a minimum of six (6) years. The copy forwarded to the Privacy Official also ~~should~~ will be maintained for six (6) years.

C. Review of Denied Access

Health Care Components are required to promptly forward requests for review of denial to a Reviewer ~~identified~~ approved by the University Privacy Official. ~~, and t~~The Reviewer is required to review the denial within a reasonable period of time, but no later than thirty (30) days after receiving the request for review. Access to Protected Health Information must be provided to the patient in accordance with the determination of the Reviewer. The Health Care Component shall notify the patient making the request ~~should be notified~~ promptly, in writing, of the Reviewer's decision, a copy of which must be filed in the patient's medical record and sent to the University Privacy Official.

IV. REFERENCES

A. HIPAA Privacy Regulations, 45 C.F. R. 164.524

UNIVERSITY OF OKLAHOMA

HIPAA Privacy Policies

Subject: Accounting of Disclosures	**Page:** 1 of 4
Policy #: Privacy-06 (Patient Rights)	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Last Revised:** January 29, 2016

I. PURPOSE

To permit patients to request an accounting of the Disclosures of their Protected Health Information.

II. POLICY*

Patients have the right to know who the University has disclosed their PHI to so each Health Care Component must record its Disclosures on an Accounting of Disclosure log. ~~The University will permit p~~Patients ~~to~~ may request a copy of this accounting.~~an accounting of Disclosures of their Protected Health Information made by the Health Care Components of the University.~~ The accounting must include Disclosures made by a Health Care Component in the six (6) years prior to the date of the request (unless limited at the request of the patient), including Disclosures to or by Business Associates.

A. Accounting Requirements – General

Each Health Care Component shall maintain an Accounting of Disclosure log on all patients. The accounting must include all Disclosures, **except** for Disclosures:

1. to carry out Treatment, Payment, or Health Care Operations;

2. to patients of Protected Health Information about them;

3. incident to a Use or Disclosure otherwise permitted or required by the Privacy Regulations (such as to Business associates or Personal Representatives);

4. pursuant to the patient's Authorization (~~s~~See Privacy-05, Patient Access to PHI);

5. for a Facility Directory, to persons involved in the patient's care, or to notify or assist in the notification of a family member, Personal Representative, or other responsible for the care of the patient of the patient's location, general condition, or death;

6. for national security or intelligence purposes;

7. to Correctional Institutions or Law Enforcement officials to provide them with

information about a person in their custody;

8. as part of a limited data set (~~s~~See Privacy-~~-~~31,~~-~~Limited Data Sets); or

9. that occurred prior to April 15, 2003.

Examples of Disclosures subject to the accounting requirement include but are not limited to Disclosures for, or pursuant to: (1) Research, unless, Authorized by patient; (2) subpoenas, court orders, or discovery requests; (3) abuse and/or neglect reporting; (4) communicable disease reporting; or (5) other reports to the Department of Health such as tumor registry.

B. Accounting Requirement – Research Involving More than 50 Participants

If, during the period covered by the accounting, a Health Care Component had made Disclosures of Protected Health Information for a particular Research purpose for 50 or more individuals, the accounting may, with respect to such Disclosures for which the Protected Health Information about the patient may have been included, provide:

1. the name of the protocol or other Research activity;

2. a description, in plain language, of the Research protocol or other Research activity, including the purpose of the Research and the criteria for selecting particular records;

3. a brief description of the type of Protected Health Information that was Disclosed;

4. the date or period of time during which such Disclosures occurred, or may have occurred, including the date of the last such Disclosure during the accounting period;

5. the name, address, and telephone number of the entity that sponsored the Research and of the researcher to whom the information was Disclosed; and

6. a statement that the Protected Health Information of the patient may or may not have been Disclosed for a particular protocol or other Research activity.

If a Health Care Component provides an accounting of Research Disclosures as provided above and if it is reasonably likely that the Protected Health Information of the patient requesting the accounting was Disclosed for such Research, the Health Care Component shall, at the request of the patient, assist in contacting the entity that sponsored the Research and the researcher.

The Research accounting provision above permits the University to meet the requirement for Research Disclosures if it provides patients with a list of all protocols for which their PHI may have been Disclosed for Research purposes pursuant to a waiver of authorization by the Privacy Board. To use this method of accounting, the Disclosure must involve at least 50 records.

C. Suspension of Accounting

A patient's right to receive an accounting of Disclosures must be suspended at the request of a Health Oversight Agency or Law Enforcement Official if certain conditions are satisfied. If a Health Care Component receives a request to suspend a patient's right to receive an accounting from a Health Oversight Agency or Law Enforcement Official, the Office of Legal Counsel or University Privacy Official ~~should~~ must be contacted to determine ~~if~~ whether the appropriate conditions have been satisfied.

III. PROCEDURE

A. A patient must request an accounting of Disclosures in writing using the Request for Accounting of Disclosure form. **Verification of the requester's identity must be obtained prior to granting the request for an accounting.** (See Privacy–03, Verification of Identity.) Health Care Components~~Patients~~ receiving a ~~making their~~ request for an accounting by telephone or e-mail ~~should~~ shall ~~be~~ forward~~ed~~ a copy of the request form or refer~~red~~ ~~to~~ the patient to the HIPAA forms webpage. The request form must be maintained in the patient's medical record for a minimum of six (6) years.

B. If a patient indicates that he/she has been treated by more than one Health Care Component, the Health Care Component that received the request ~~should~~ shall immediately forward a copy of the request to the University Privacy Official, who will coordinate the processing of the request with the other University Health Care Components designated by the patient. If the patient does not request an accounting from any other Health Care Components, the Health Care Component that received the initial request ~~should~~ shall process the request in accordance with its internal procedures and send a copy of the request form and a copy of the accounting of Disclosure log to the University Privacy Official, upon request.

C. Health Care Components must designate and document the title(s) of the ~~an~~ individual or ~~individuals who will~~ office ~~be~~ responsible for receiving and processing requests for accountings of Disclosures. A copy of the designations must be provided to the University Privacy Official upon request. The Health Care Components must update the list as changes are made and provide the updated list to the University Privacy Official, who will maintain a copy of the designation for a minimum of six (6) years.

D. For each Disclosure that must be recorded, the accounting log must include the following information:

1. the date of the Disclosure;

2. the name of the entity or person who received the Protected Health Information and, if known, the address of such entity or person;

3. a brief description of the Protected Health Information that was Disclosed; and

4. a brief statement of the purpose of the Disclosure that reasonably informs the patient of the basis for the Disclosure, or a copy of the written request for the Disclosure~~,~~

~~if approved by the University Privacy Official~~.

E. An Accounting of Disclosure log must be used to record Disclosures and must be maintained in a patient's medical record for a period of at least six (6) years from that date of the last accounting.

F. The Request for Accounting of Disclosures form and the log forwarded to the Privacy Official also should be maintained for six (6) years.

G. If during the period covered by the accounting a Health Care Component has made multiple Disclosures of Protected Health Information to the same person or entity for a single purpose, or pursuant to a single Authorization, the accounting may, with respect to such multiple Disclosures ~~and upon approval of the University Privacy Official~~, provide:

1. the information set forth in section 4 above for the first Disclosure during the accounting period;

2. the frequency, periodicity, or number of the Disclosures made during the accounting period; and

3. the date of the last such Disclosure during the accounting period.

H. If during the period covered by the accounting the Health Care Component has used a Business Associate, the Health Care Component must contact the Business Associate to obtain an Accounting of Disclosures made by the Business Associate. This accounting must also be provided to the patient.

I. The Health Care Component will act on the patient's request for an accounting no later than sixty (60) calendar days after receipt of such a request. If the Health Care Component is unable to meet this deadline, it must contact the University Privacy Official to request an extension, which may not exceed 30 calendar days. The University Privacy Official will be responsible for contacting the patient regarding any necessary extension.

J. The first accounting to a patient in any twelve-month period must be provided at no charge. The University may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same patient within the twelve-month period, provided that the University informs the patient in advance of the fee and provides the patient with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee. (See Privacy-05, ~~-~~Patient Access to Protected Health Information for information about fees.)

IV. REFERENCES

A. HIPAA Privacy Regulations, 45 C.F. R. 164.528

UNIVERSITY OF OKLAHOMA

HIPAA Privacy Policies

Subject: Communication by Alternative Means	**Page:** 1 of 2
Policy #: Privacy-07 (Patient Rights)	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Revised:** January 29, 2016

I. PURPOSE

To permit patients to request communication of Protected Health Information by alternative means or at alternative locations.

II. POLICY*

The University will permit patients to request, and will accommodate reasonable requests by patients, to receive communications of Protected Health Information by alternative means or at alternative locations.

If a request for communication by alternative means is granted, Health Care Components of the University must communicate with the patient in accordance with the granted request.

The University **cannot** require an explanation from the patient as to the basis for the request as a condition of considering or granting the request.

The University can condition the ~~provision~~ acceptance of an alternative means of communication on receiving: (a) information as to how payment will be handled, if applicable and (b) the specification of an alternative address or other method of contact.

III. PROCEDURE

A. A patient must request communication by alternative means or at alternative locations in writing by using the Request for Communication by Alternative Means form (available on the HIPAA forms web page).

B. Any Health Care Component that receives a request from a patient to receive communications by alternative means or at alternative locations ~~should~~ shall provide the patient with the Request for Alternative Communication form. If a patient indicates that he/she has been treated by more than one Health Care Component and wants the request to apply those Health Care Components as well, the Health Care Component that received the request ~~should~~ shall immediately forward a copy of the request to the University Privacy Official, who will coordinate the processing of the request with the other University Health Care Components designated by the patient.

*Capitalized terms are defined in Privacy-01, Definitions

If the patient does not request an alternative means of communication from any other Health Care Components, the Health Care Component that received the initial request ~~should~~ shall process the request in accordance with its internal procedures and send a copy of the request form and the denial form, if applicable, to the University Privacy Official upon request.

~~3~~C. Health Care Components must designate and document the title(s) of the individual or office responsible for receiving and processing requests for alternative methods of communication. A copy of the designations must be provided to the University Privacy Official upon request. The Health Care Components must update the list as changes are made and provide the updated list to the University Privacy Official, who will maintain a copy of the designation for a minimum of six (6) years. ~~Health Care Components must designate an individual or individuals who will be responsible for determining if a particular request for alternative means of communication is reasonable in light of any expense and administrative burden involved with complying with the request.~~ Questions regarding the reasonableness of a particular request should be discussed with the University Privacy Official.

~~4~~D. If~~A~~ a patient ~~who~~ makes a request in writing at the time of an office visit, the HCC should notify the patient of the denial, if the request is denied during the same office visit. The patient ~~should~~ shall be provided with a copy of the Request form with the reason for the denial noted. If the patient cannot be notified of the denial at the time of his/her visit, the Request form, with the denial noted, ~~should~~ must be sent to the patient. **In order to protect the patient, the denial ~~should~~ must be sent to the alternative address, if one was specified, for this communication only.**

~~5~~E. Requests for alternative means of communication and documentation of any denials of such requests ~~should~~ shall be maintained in a patient's medical record for a minimum of six (6) years.

~~6~~F. The agreed upon alternative means of communication ~~should~~ must be communicated to the billing department and other departments, providers, and Business Associates who may be ~~sending the patient~~ communicati~~n~~g~~on~~ with the patient on behalf of the Health Care Component that agreed to the request. Health Care Components must send those departments and entities a copy of the approved Request form.

~~7~~G. **If a request for communication by alternative means is granted, a Health Care Component must place a clear indication of the alternative communication by means on or in the patient's medical record, to ensure the alternative means is observed. Failure to observe the alternative communication means may result in a HIPAA violation.**

IV. REFERENCES

A. HIPAA Privacy Regulations, 45 C.F.R. 164.522 (b)

UNIVERSITY OF OKLAHOMA

HIPAA Privacy Policies

Subject: Right to Amend Records	**Page:** 1 of 3
Policy #: Privacy-08 (Patient Rights)	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Last Revised:** January 29, 2016

I. PURPOSE

To permit patients to request amendments to their Protected Health Information.

II. POLICY*

The University will permit patients to request amendments to their Protected Health Information contained in a Designated Record Set. (See Privacy-01, Definitions.)

A. The University may deny a patient's request for amendment if it determines that the Protected Health Information or record that is the subject of the request:

~~A~~1. Was not created by University Personnel, unless the patient provides a reasonable basis to believe that the originator of Protected Health Information is no longer available to act on the requested amendment;

~~B~~2. is not part of the Designated Record Set;

~~C~~3. is not available for inspection by the patient pursuant to Privacy-05, Patient Access to Protected Health Information Policy;

~~D~~4. is accurate and complete.

B. Patients requesting an amendment to their Protected Health Information must provide a reason to support a requested amendment. ~~. (See~~ using the Request for Amendment of PHI form, available on the HIPAA website.~~)~~

C. Health Care Component that is informed by another Covered Entity of an amendment to a patient's Protected Health Information must amend the Protected Health Information in its Designated Record Sets.

III. PROCEDURE

A. Patients must request amendments to their Protected Health Information in writing by using the University's Request for Amendment of Protected Health Information form. Health Care Components that receive a ~~Patients making their~~ request for an amendment by telephone or e-mail ~~should be sent~~ must send the patient a copy of the form or refer~~red~~ the patient to the HIPAA forms webpage. Verification of the requester's identity must be obtained prior to

*Capitalized terms are defined in Privacy-01, Definitions

considering the amendment request. (See Privacy-03, Verification of Identity.) The request form must be maintained in the patient's medical record for a minimum of six (6) years.

B. If a patient indicates on the form that he/she has been treated by more than one Health Care Component and the requested amendment affects those Health Care Components, the Health Care Component that received the request ~~should~~ shall immediately forward a copy of the request to the University Privacy Official, who will coordinate the processing of the request with the other University Health Care Components designated by the patient. If the patient does not request an amendment from any other Health Care Component, the Health Care Component that received the initial request ~~should~~ shall process the request in accordance with its internal policy and file a copy of the request in the patient's medical record.

C. Health Care Components must designate and document the title(s) of the individual or office responsible for receiving and processing requests for amendment. A copy of the designations must be provided to the University Privacy Official upon request. The Health Care Components must update the list as changes are made and provide the updated list to the University Privacy Official, who will maintain a copy of the designation for a minimum of six (6) years. ~~Health Care Components should designate an individual or individuals who will be responsible for processing a particular amendment request.~~ The specific provider responsible for recording the Protected Health Information or originating the record must be consulted, if possible, and should sign the amendment form.

D. Health Care Components must act on the patient's request no later than sixty (60) calendar days after receipt of a request, as set forth below:

1. Accepting the Amendment. If the Health Care Component accepts the requested amendment, in whole or in part, the Health Care Component must: (i) make the appropriate amendment by identifying the records in the Designated Record Set that are affected by the amendment and appending or providing a link to the amendment to that record; (ii) inform the patient, in writing, that the amendment is accepted by sending the patient a copy of the Request for Amendment Acceptance form with the acceptance noted; (iii) obtain the patient's identification of and agreement to have the Health Care Component notify the relevant persons with whom the amendment needs to be shared (usinge the Request form); and (iv) make reasonable efforts to provide the amendment within a reasonable time to persons identified by the patient as having received Protected Health Information about the patient and needing the amendment, and persons as well as Business Associates that the Health Care Component knows have the Protected Health Information that is the subject of the amendment and who may have relied, or could foreseeably rely, on such information to the detriment of the patient.

2. Denying the Amendment. If the Health Care Component denies the requested amendment, in whole or in part, the Health Care Component must: (i) inform the patient, in writing, that the amendment is denied by sending the patient a copy of the Denial form; (ii) permit the patient to submit to the Covered Entity a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement; (iii) identify, as appropriate, the record or Protected Health Information in the Designated Record Set that is the subject of the disputed amendment and append or otherwise link the patient's request for an amendment; the Health Care Component's denial of the request; the patient's statement of disagreement, if any; and the Health Care Component's rebuttal, if any, to the Designated Record Set. (A Health Care Component may, but is not required to, prepare a written rebuttal to the patient's statement of disagreement. If a rebuttal statement is prepared, a copy ~~of it~~ must be

provided to the patient who submitted the statement of disagreement.) The University Privacy Official must be contacted prior to sending the rebuttal.

E. If a statement of disagreement has been submitted by the patient, a Health Care Component must include the material set forth in subsection (D)(2)(iii) of the preceding paragraph or, at the election of the Health Care Component, an accurate summary of any such information, with any subsequent Disclosure of the Protected Health Information to which the disagreement related.

F. If the patient has not submitted a written statement of disagreement, the Health Care Component must include the patient's request for amendment and its denial, or an accurate summary of such information, with any subsequent Disclosure of the Protected Health Information **only if the patient has requested such action**.

~~G A Health Care Component that is informed by another Covered Entity of an amendment to a patient's Protected Health Information must amend the Protected Health Information in its Designated Record Sets.~~

~~H~~G. Requests for amendments and documentation of the response to such requests must be maintained in a patient's medical record for a minimum of six (6) years.

IV. REFERENCES

A. HIPAA Privacy Regulations, 45 C.F.R. 164.526 (a)~~.~~

UNIVERSITY OF OKLAHOMA

HIPAA Privacy Policies

Subject: Right to Request Restriction on Use and Disclosures	**Page:** 1 of 3
Policy #: Privacy-09 (Patient Rights)	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Last Revised:** January 29, 2016

I. PURPOSE

To permit patients to request certain restrictions on the Use and Disclosure of their Protected Health Information.

II. POLICY *

The University will permit patients to request restrictions on the Use and Disclosure of their Protected Health Information: (a) to carry out Treatment, Payment, or Health Care Operations and/or (b) to people involved in their care or for notification purposes as described in Privacy-26, Disclosures to Family and Others.~~§ 164.510(b) of the Privacy Regulations.~~ **However, the University is not required to agree to any request to restrict the Use and Disclosure of Protected Health Information, unless (a) the Disclosure is to a H~~h~~ealth p~~P~~lan for purposes of Payment or Health Care Operations; and (b) the PHI pertains to a health care item or service for which the ~~provider has been paid out-of-pocket in full by the patient or other payer, such as a family member~~patient or individual on behalf of the patient (such as a family member) has paid the University in full.**

If the University agrees to a restriction, it may not Use or Disclose Protected Health Information in violation of the restriction, except in emergency situations when the Protected Health Information is needed to treat the patient. If restricted Protected Health Information is Disclosed to a Health Care Provider for emergency treatment, the Health Care Component disclosing the information must request that the Health Care Provider who received the information not to further Use or Disclose the information.

Any agreed-upon restriction will not be effective to prevent Uses and Disclosures to the patient or as Required by Law.

The University must adhere to any agreed-upon restriction until the restriction is terminated according to the procedures set forth below.

University Personnel may not Use or Disclose Protected Health Information that is subject to a restriction, except to provide emergency treatment or as Required by Law.

III. PROCEDURE

A. Patients must request restrictions on the Use and Disclosure of their Protected Health Information in writing by using the Request for Restriction on Use and Disclosures of Protected Health Information form. Health Care Components shall send a copy of the form to p~~P~~atients making their restriction requests by telephone or e-mail ~~should be sent a copy of the form~~ or refer~~red~~ them to the HIPAA forms webpage. Verification of the requester's identity must be obtained prior to considering the request. (See Privacy-03, Verification of Identification.)

B. Any Health Care Component that receives a restriction request ~~should~~ shall provide the patient with the Request for Restriction form. If a patient indicates on the form that he/she has been treated by more than one Health Care Component and wants the restriction to apply to those Health Care Components, the Health Care Component that received the request ~~should~~ shall immediately forward a copy of the request to the University Privacy Official, who will coordinate the processing of the request with the other Health Care Components designated by the patient. If the patient does not request a restriction on the use of Protected Health Information created or maintained by any other Health Care Components, the Health Care Component that received the initial request ~~should~~ shall process the request in accordance with its internal procedures and file a copy of the request form in the patient's medical record.

C. Health Care Components must designate and document the title(s) of the individual or office responsible for receiving and processing requests for restrictions. A copy of the designations must be provided to the University Privacy Official upon request. The Health Care Components must update the list as changes are made and provide the updated list to the University Privacy Official, who will maintain a copy of the designation for a minimum of six (6) years.
~~Health Care Components must designate an individual or individuals who will be responsible for determining if a particular restriction will be permitted.~~

Requests for restrictions that are not Required by Law to be granted should generally be granted only in rare instances in which the facts and circumstances indicate such a restriction is necessary to protect the patient.

D. The Privacy Official should be contacted prior to agreeing to any restriction request.

E. Health Care Components must notify the patient in writing if the request is denied by providing the patient with a copy of the completed Request for Restriction form that includes the reason for the denial. If the patient cannot be notified of the denial at the time of his/her next visit, the form, with the denial noted, ~~should~~ must be sent to the patient.

F. Requests for restrictions and documentation of approvals or denials of such requests shall be maintained in a patient's medical record for a minimum of six (6) years.

G. The agreed-upon restrictions on the Use and Disclosure of Protected Health Information should be communicated to the billing department and other departments, providers, and Business Associates who may be Using or Disclosing the patient's Protected Health Information

on behalf of the University and/or Health Care Component that agreed to the request. Health Care Components must send those departments and entities a copy of the approved Request form.

H. A restriction on the Use and Disclosure of Protected Health Information that has been granted but is not Required by Law can be terminated if (a) the patient requests the termination in writing; (b) the patient orally agrees to or requests the termination and the oral request or agreement is documented in the patient's medical record and communicated in writing to the Privacy Official; or (c) the University and/or the Health Care Component informs the patient that it is terminating its agreement to the voluntary restriction, in which case the termination will apply only to Protected Health Information created or received after the patient has been notified of the termination. The Revocation of Request for Restriction and Use and Disclosure of PHI form, available on the HIPAA website, may be used.

I. **If a restriction request is granted, a Health Care Component must place a clear indication of the restriction on or in the patient's medical record, to ensure the restricted information is not inadvertently made available. Failure to comply with the granted restriction may result in a HIPAA violation.**

IV. REFERENCES

A. HIPAA Privacy Regulations, 45 C.F. R. 164.522 (a)

UNIVERSITY OF OKLAHOMA

HIPAA Privacy Policies

Subject: Privacy Official – Designation	**Page:** 1 of 1
Policy #: Privacy-10 (Admin.)	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Last Revised:** January 29, 2016

I. PURPOSE

To provide for the designation of a Privacy Official and to set forth contact information as required by the Privacy Regulations.

II. POLICY*

The Board of Regents shall designate a Privacy Official who is responsible for the development and implementation of the University's Privacy Policies for its Health Care Components and who will be responsible for answering questions regarding the content of the University's Privacy Policies and Notice of Privacy Practices. The Privacy Official also will be responsible for receiving, coordinating, and managing the investigation of complaints regarding HIPAA compliance.

III. PROCEDURE

A. Documentation regarding the designation of the Privacy Official and his/her contact information must be retained, in written or electronic format, for at least six (6) years by the University Privacy Official.

B. The contact information for the University Privacy Official is set forth on the University's Office of Compliance and HIPAA web pages and will be revised in the event a new University Privacy Official is designated or the contact information changes.

IV. REFERENCES

A. HIPAA Privacy Regulations, 45 C.F.R. 164.530.

UNIVERSITY OF OKLAHOMA

HIPAA Privacy Policies

Subject: Privacy Complaint Reporting and Tracking	**Page:** 1 of 2
Policy #: Privacy-11 (Admin.)	**Approved:** July 30, 2008
Effective Date: August 1, 2008	**Last Revised:** January 29, 2016

I. PURPOSE

To establish the procedures for documenting and tracking ~~individuals to submit~~ complaints filed by individuals about HIPAA policies, procedures, and incidents regarding ~~the~~ alleged failures to comply with the University's Privacy Policies by the University's Health Care Components and/or University Personnel.

II. POLICY*

All incidents regarding the alleged failure to comply with the University's HIPAA Policies and compliance with such Policies, regardless of the form in which they are reported, ~~will~~ must be documented, reviewed, and acted upon, if necessary, by the University's Privacy Official or designee. Health Care Components may ask but may not require that complaints be reported on the University's HIPPA Privacy Complaint form.

Documentation regarding incident reports received and the resolution of such complaints will be retained, in written or electronic format, for at least six (6) years.

III. PROCEDURE

A. Each Health Care Component shall designate and document an individual responsible for receiving and managing Privacy incidents involving the Health Care Component.

Each Health Care Component must develop and implement a process for receiving these reports, reporting them immediately to the University's Privacy Official, and investigating them in coordination with the University Privacy Official. Such process can be as simple as notifying employees that each individual reporting a Privacy-related incident should be instructed to contact the University's Privacy Official or the Health Care Component's designee. The contact information for the University's Privacy Official is located on the University's Office of Compliance and HIPAA web pages.

Each Health Care Component shall track Privacy incident reports received using a process that involves the notification of the University's Privacy Official of each report received so that the University Privacy Official can also record and track the investigation and response to each report and can participate in the resolution.

B. The University Privacy Official will be responsible for the investigation of each report, in coordination with or through the appropriate Health Care Component and, if necessary, with other affiliated entities. The individual in the Health Care Component designated to receive

Privacy incident reports shall manage the investigation at the request of the University Privacy Official.

C. The Health Care Component and the University Privacy Official shall each maintain a record of each Privacy incident, the investigation, and the resolution. The Health Care Component shall provide a copy of this record to the University Privacy Official upon request and at least annually.

IV. REFERENCES

A. HIPAA Privacy Regulations, 45 CFR §164.530(d).

UNIVERSITY OF OKLAHOMA

HIPAA Privacy Policies

Subject: Documentation	**Page:** 1
Policy #: Privacy-12 (Admin.)	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Last Revised:** January 29, 2016

I. PURPOSE

To establish documentation requirements as required by the Privacy Regulations.

II. POLICY*

The University and each Health Care Component, as appropriate, will maintain, for at least six (6) years, the following:

A. Written or electronic copies of its Privacy Policies;

B. Written or electronic copies of any communication that is required by the Privacy Regulations to be in writing; and

C. Written or electronic ~~records~~ copies of any action, activity, or designation that is required by the Privacy Regulations to be documented.

III. PROCEDURE

A. Documentation of Privacy Policies. Written or electronic copies of the University's Privacy Policies will be maintained by the University Privacy Official for at least six (6) years from the date the Policies were created or were last in effect, whichever is later.

B. Documentation of Communications Required by the Privacy Regulations. This documentation will be retained for a period of at least six (6) years from the date of creation, as specified in the related Privacy Policy. For example: The Policy addressing the right of patients to have access to their Protected Health Information (Privacy-05) states that the Authorization form must be maintained in ~~a~~ the patient's medical record for a minimum of six (6) years.

C. Documentation of Any Action, Activity, or Designation Required by Privacy Regulations. This documentation will be retained for a period of at least six (6) years from the date of creation, as specified in the related Privacy Policy. For example: The Policy addressing the appointment of a Privacy Official (Privacy-10) specifies that the designation of the Privacy Official will be maintained by the University Privacy Official, in written or electronic format, for at least six (6) years.

Health Care Components should contact the University Privacy Official prior to destroying any HIPAA-related documentation to ensure compliance with this policy.

IV. REFERENCES

A. HIPAA Privacy Regulations, 45 C.F.R. 164.530 (j).

*Capitalized terms are defined in Privacy-01, Definitions

UNIVERSITY OF OKLAHOMA

HIPAA Privacy Policies

Subject: Retaliation and Intimidation	**Page:** 1 of 2
Policy #: Privacy-13 (Admin.)	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Last Revised:** January 29, 2016

I. PURPOSE

To prohibit retaliation and intimidation against individuals who exercise their rights under the Privacy Regulations.

II. POLICY*

The University, its Health Care Components, and University Personnel shall not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against an individual for:

A. Exercising any right under, or for participating in, any process established by the Privacy Regulations;

B. Filing a complaint with the Secretary of the Department of Health and Human Services as permitted by the Privacy Regulations;

C. Testifying, assisting, or participating in an investigation, compliance audit or review, proceeding, or hearing conducted by the University or a government enforcement agency under the Privacy Regulations; or

D. Opposing any act or practice made unlawful by the Privacy Regulations, provided the individual has a good faith belief that the practice opposed is unlawful and the manner of the opposition is reasonable and does not involve a Disclosure of Protected Health Information in violation of the Privacy Regulations or the University's Privacy Policies.

For purposes of this Policy, the term "individual" is not limited to natural persons, but includes any type of organization, association, or group such as other Covered Entities, Health Oversight Agencies, and advocacy groups.

III. PROCEDURE

A. Any individual who believes that some form of retaliation or intimidation against an individual for exercising rights under the Privacy Regulations is occurring or has occurred should report the incident to the University Privacy Official.

B. If the University Privacy Official receives a report of retaliation or intimidation, the University Privacy Official will conduct an investigation to determine if retaliation or intimidation has occurred. If the report is substantiated, sanctions will be imposed in accordance with University and Privacy Policies.

C. If the individual believes the University Privacy Official has retaliated against or intimidated him, the individual should report the incident to the University's Director of Compliance at 405-271-2511.

IV. REFERENCES

A. ~~A.~~ HIPAA Privacy Regulations, 45 CFR 164.530(g).
~~A.~~B. HIPAA Privacy Regulations, ~~and~~ 45 CFR 160.316.

UNIVERSITY OF OKLAHOMA

HIPAA Privacy Policies

Subject: Mitigation	**Page:** 1 of 1
Policy #: Privacy-14 (Admin.)	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Last Revised:** January 29, 2016

I. PURPOSE

To establish procedures regarding the mitigation of harmful effects of inappropriate Uses or Disclosures of, or access to Protected Health Information.

II. POLICY*

The University will mitigate, to the extent practicable, any harmful effect that is known to the University of a Use or Disclosure of ~~or access to~~ Protected Health Information in violation of the University's Privacy Policies or the Privacy Regulations by the University, one of its Health Care Components, University Personnel, or a Business Associate of the University.

III. PROCEDURE

A. Health Care Components must take practicable steps to mitigate the harmful effects of inappropriate Use or Disclosure of ~~or access to~~ Protected Health Information. The type of mitigation that occurs will be based on the facts and circumstances of each case, ~~based on~~taking into consideration the following factors:

1. knowledge of where the Protected Health Information has been Disclosed~~; or accessed;~~
2. how the Protected Health Information that was improperly accessed, Used, or Disclosed might be used to cause harm to the patient or another individual; and
3. what steps can actually have a mitigating effect under the facts and circumstances of the specific situation.

B. Health Care Components must, in coordination with the University Privacy Official, investigate the cause of the inappropriate ~~access,~~ Use~~,~~ or Disclosure and take corrective actions to prevent such from ~~re-occurring~~recurring.

C. Health Care Components shall notify the University Privacy Official, in accordance with Privacy-11, Privacy Complaint Reporting and Tracking, of inappropriate ~~access,~~ Uses~~,~~ and Disclosures; the results of the investigation; and the proposed mitigation efforts. Once mitigation is determined, the Health Care Component must confirm it is implemented.

D. If legal action is threatened or is a distinct possibility~~,~~ as a result of the harmful effect, the Health Care Component must notify the Office of Legal Counsel ~~must be notified~~.

IV. REFERENCES

A. HIPAA Privacy Regulations, 45 CFR 164.530(f).

*Capitalized items are defined in Privacy-01, Definitions

UNIVERSITY OF OKLAHOMA

HIPAA Privacy Policies

Subject: Development and Amendment of Privacy ~~Practices and Policies~~Policies and Procedures	**Page:** 1 of 2
Policy #: Privacy-15 (Admin.)	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Last Revised:** January 29, 2016

I. PURPOSE

To outline the requirements for the development and amendment ~~changes~~ to the University's ~~Notice of~~ Privacy ~~Practices~~ policies and procedures, including related ~~and amendment of its Privacy Policies and~~ forms.

II. POLICY*

The University, through its Privacy Official, will implement policies and procedures with regard to PHI that are designed to comply with the HIPAA regulations. It shall ~~promptly change its Notice of Privacy Practices and~~ amend its Privacy Policies, procedures, and related forms as necessary and appropriate to comply with changes in the law, including the Privacy Regulations; ~~, or~~ to accommodate changes in the structure or operations of the University or its Health Care Components; and when otherwise necessary and appropriate.

The University has reserved, in its Notice of Privacy Practices, the right to change its Privacy practices and amend its Privacy Policies. Therefore, any such changes or amendments will be effective for Protected Health Information created or received by the University or its Health Care Components ~~after~~ prior to the effective date of the amendment. If any such changes affect the content of the Notice of Privacy Practices, the University, through its Privacy Official, shall promptly amend its Notice of Privacy Practices.

III. PROCEDURE

A. Changes to Privacy Practices and Policies Addressed in the Notice of Privacy Practices. In order to effectuate changes to Privacy ~~practices and~~ Policies and procedures addressed in the Notice of Privacy Practices, the University through its Privacy Official, will:

1. Ensure that the Privacy Policies, if revised to reflect a change in the University's Privacy practices, comply with the Privacy Regulations and applicable state laws that are not preempted.

2. Document the revised Privacy Policy, in written or electronic format, and retain such documentation for at least six (6) years.

3. Revise the University's Notice of Privacy Practices as required by the Privacy Regulations to state the changed practice and make the revised Notice available as required.

B. Amendments to Privacy Policies Not Addressed in the Notice of Privacy Practices. The University may amend, at any time, a Privacy Policy that does not materially affect the content of its Notice of Privacy Practices. In order to implement such an amendment, the University, through its University Privacy Official, will:

1. Ensure that the Privacy Policy, as amended, complies with the Privacy Regulations; and

2. Document the revised Privacy Policy, in written or electronic format, and retain such documentation for at least six (6) years.

IV. REFERENCES:

A. HIPAA Privacy Regulations, 45 C.F.R. 164.530(i).

UNIVERSITY OF OKLAHOMA

HIPAA Privacy Policies

Subject: Waiver of Rights	**Page:** 1 of 1
Policy #: Privacy-16 (Admin.)	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Last Revised:** January 29, 2016

I. PURPOSE

To prohibit requiring patients to waive their rights under the Privacy Regulations.

II. POLICY*

The University will not require patients to waive (a) their right to file a complaint with the Secretary of the Department of Health and Human Services or any other enforcement agency regarding the University's compliance with the Privacy Regulations or (b) any other rights under the Privacy Regulations as a condition of Treatment or Payment Activities.

III. PROCEDURE

A. Any person with knowledge of a violation of this Policy ~~should~~ shall promptly report the incident to the University Privacy Official.

B. If the University Privacy Official receives a report of a violation of this Policy, the University Privacy Official will conduct an investigation to determine if a violation has occurred. If the report is substantiated, sanctions will be imposed pursuant to Privacy-19, Sanctions.

IV. REFERENCES

A. HIPAA Privacy Regulations, 45 C.F. R. 164.530(h).

UNIVERSITY OF OKLAHOMA

HIPAA Privacy Policies

Subject: Training - Privacy	**Page:** 1 of 4
Policy #: Privacy-17 (Admin.)	**Approved:** July 1, 2009
Effective Date: July 1, 2009	**Last Revised:** January 29, 2016

I. PURPOSE

To provide for training regarding the University's HIPAA Privacy Policies and procedures.

II. POLICY*

University Workforce Members associated with Health Care Components shall take the University's HIPAA Privacy training annually, as provided in this policy. In addition, training shall be provided to affected Workforce Members by the University Privacy Official or Health Care Component within a reasonable period of time after material changes to HIPAA or University policies and procedures are made.

On the Health Sciences Center campus, individuals who must take annual training are all volunteers, employees, and University students/trainees. On the Norman campus, those individuals are all volunteers, employees, and University students/trainees in a designated Health Care Component.

Employees include any person whose conduct is under the direct control of the Health Care Component, such as temporary employees and float pool staff.

Health Care Components may impose additional training requirements on their Workforce Members but may not waive any of the training requirements in this policy.

III. PROCEDURE

A. Program. The University, through the Privacy Official and committee(s) established by the Privacy Official, will direct the methods and manner in which the University's Privacy training will be accomplished. (See the HIPAA Security Training policy for the HIPAA Security Training requirements.)

B. Materials. Training materials should include a test or some other opportunity to demonstrate understanding of the information presented. Training must be completed according to the standards in this Policy in order for the training requirement to be satisfied.

C. Tracking. It is the responsibility of each Health Care Component, in coordination with

the Office of Compliance and/or Human Resources Office, to ensure that its employees, volunteers, and University students/trainees ~~receive~~ complete training according to the University's HIPAA Privacy Policies.

1. A Privacy Training Coordinator, or Coordinators, should be designated by each Health Care Component to coordinate with the Office of Compliance and/or Human Resources Office to ensure that training is accomplished according to the University's HIPAA Privacy Policies.

2. Training will be tracked by utilizing PeopleSoft or an equivalent system, with the assistance of the University's Compliance, Human Resources, and Student Affairs or Admissions offices. If requested, the University's Human Resources and Student Affairs or Admissions offices will provide reports to the Office of Compliance or designee indicating the names of new employees, volunteers, and University students/trainees and the Health Care Component/department, if applicable, with which they will be associated.

D. Timing. Each new employee, volunteer, and University student/trainee must complete the University's online HIPAA Privacy training as provided below.

1. Regular Employees must complete the University's online HIPAA Privacy training within 30 days of becoming an employee. Health Care Components must also provide a written or oral review of their specific HIPAA Privacy policies and procedures relevant to the employee's duties as soon as reasonably possible.

2. Temporary Employees must complete the University's HIPAA Privacy training if they are expected to work for a Health Care Component for more than 5 consecutive days[**]. Training must be completed on or before the 6th day of providing services to the Health Care Component and may be completed online or on a printed version of the online course. Documentation of training must be maintained by the Health Care Component. In addition, the Health Care Component must provide a review of its specific ~~relevant~~ HIPAA Privacy policies relevant to the temporary employee's duties as soon as reasonably possible.

   Temporary employees providing fewer than 6 consecutive days of services may be required by the Health Care Component to take the University's HIPAA Privacy training. The Health Care Component must, at a minimum, provide these individuals a review of ~~applicable~~ HIPAA Privacy policies and procedures applicable to their duties as soon as reasonably possible.

   Temporary Employees are required to execute the University's Confidentiality Agreement (available on the University's HIPAA website). The Health Care Component shall maintain that Agreement for at least six (6) years, or ~~for as long as~~longer if required by other University policies.

3. Volunteers (excluding volunteer faculty) must complete the University's HIPAA Privacy training if they are expected to volunteer for a Health Care Component for

[**] Health Care Components should give consideration to the length of temporary employment or volunteer position when determining how soon after the first day the individual must complete the training.

more than 5 consecutive ~~days~~[1] days.[**] ~~.~~ Training must be completed on or before the 6th day of providing volunteer services and may be completed online or on a printed version of the online course. In addition, the Health Care Component must provide a review of its ~~relevant~~ HIPAA Privacy policies and procedures applicable to the volunteer's duties as soon as ~~is~~ reasonably possible.

Volunteers providing fewer than 6 consecutive days of volunteer services may be required by the Health Care Component to take the University's HIPAA Privacy training. The Health Care Component must, at a minimum, provide these volunteers a review of ~~applicable~~ HIPAA Privacy policies and procedures applicable to the volunteer's duties as soon as reasonably possible.

Volunteers (excluding faculty) must sign the University's Confidentiality Agreement (available on the University's HIPAA forms page). The Health Care Component shall maintain the Agreement for at least 6 years, or ~~for as~~ longer ~~as~~ if required by other University policies.

4. Volunteer F~~f~~aculty may substitute annual HIPAA training received at another entity for the annual University HIPAA Privacy training if their Health Care Component verifies that they (~~1~~a) do not have access to the University's network, and (~~2~~b) do not provide their volunteer services at an OU facility or clinic, and (~~3~~c) do not access OU patients or their PHI in their volunteer capacity. The~~se~~ volunteer faculty~~s~~ must certify each year to the ~~department~~ Health Care Component Privacy Training Coordinator ~~designated for the Health Care Component~~ that they have received annual HIPAA training elsewhere. The Health Care Component is responsible for maintaining these certifications and providing them to the Office of Compliance or University Privacy Official upon request.

5. Enrolled University Students/Trainees must complete training in accordance with D.1 above.

6. Visiting Students/~~ and~~ Trainees may show proof of HIPAA Privacy training from their home institution (a copy of which must be maintained by their Health Care Component) or take the University's Privacy training in accordance with D.3. Health Care Components must also provide a review, as stated in D.3 above.

7. Others - Health Care Components must contact the University Privacy Official to determine the training requirements for any other individuals.

E. Material Changes. The University Privacy Official or Health Care Component will provide training to those W~~w~~orkforce ~~m~~Members whose job or academic functions are affected by a material change in the University's Privacy Policies within a reasonable period of time after the change becomes effective.

F. Sanctions**.** Employees who fail to complete the training are subject to sanctions pursuant to Privacy-19, Sanctions. Students who fail to complete training will not be permitted to enroll for the next semester or session. Temporary employees, ~~trainees/~~visiting students/trainees, and volunteers, including volunteer faculty, who fail to complete annual training will not be permitted to provide services to or continue training at the University.

G. Documentation. Documentation regarding training must be maintained by the Health Care Component/department ~~and the Office of Compliance~~, in written or electronic format, for at least six (6) years, or ~~for as long as~~longer if required by other applicable University policies.

H. Compliance Assistance. Health Care Components or Privacy Training ~~c~~Coordinators having difficulty with individual employees, volunteers, or University or visiting students/trainees complying with the training requirements should contact the Office of Compliance or appropriate dean or vice president for assistance.

IV. REFERENCES

A. HIPAA Privacy Regulations, 45 CFR §164.530(b).
B. HIPAA Privacy Policy, Sanctions-19.
C. Confidentiality Agreement – HIPAA Privacy forms page.

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:** January 29, 2016

I. PURPOSE

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

II. POLICY*

The University, through its Health Care Components, will implement appropriate administrative, technical, and physical safeguards that will reasonably protect ~~safeguard~~ 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.

~~**University Personnel 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 ~~other~~ 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 ~~Official~~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 ~~in ear shot~~present. Patient identifying information should be Disclosed during oral conversations only when necessary for Treatment, Payment, teaching, Research, or Healthcare Operation~~sal~~ 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.

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 Privacy-07, Communication by Alternative Means.) PHI should not be left in a telephone message. Telephone messages ~~regarding test results or~~ that contain information that links a patient~~'s name~~ 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.

~~2.~~3. Faxes. The following procedures must be followed when faxing PHI:

   a. Only the PHI necessary to meet the authorized requester's needs may be faxed.

   b. Each Health Care Component ~~should designate employees~~ must provide training to Workforce Members who ~~can~~ will fax, or approve the faxing of, PHI. ~~Unauthorized employees, students, and volunteers should not fax PHI.~~

   c. Unless otherwise permitted or Required by Law, a properly completed and signed Authorization must be obtained before ~~releasing~~ 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.)

   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 ~~should~~ 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.

   f. Fax machines must be located in secure areas not readily accessible to visitors or patients to protect incoming and outgoing PHI. ~~Incoming f~~Faxes containing PHI must not be left sitting on or near the machine for extended periods of time.

g. 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.

h. 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; and Privacy-06, Accounting of Disclosures; as well as any internal Health Care Component reporting requirements and the envelope is sealed.

~~3.~~4. Mail. PHI may be mailed within the University if placed in sealed envelopes or locked mail bags. PHI, includinge appointment reminders, may be mailed outside the University if the contents are concealed.

~~4.~~5. ~~Copying~~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.

~~5.~~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.

~~6.~~7. 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 it cannot be read or reconstructed. Health Care Components are encouraged to 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 the University Electronic Data Disposal and Reuse policy (available from IT Security.) Hard drives and other electronic devices shall be destroyed or managed in accordance with IT 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 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 ~~concealed when not in use to avoid~~positioned in a manner that prevents access by unauthorized persons. Paper records shall be secured when the area is unattended.

a. Storage. Paper records s 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. ~~University employees~~ **Workforce Members shall not remove documents containing PHI from the University premises solely for their ~~own~~ convenience.** Workforce Members may remove such documents~~They may not be removed~~ from University premises ~~unless~~ when necessary for Treatment, Payment, or Operations ~~to a patient~~ 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 ~~and~~ or procedures and must be returned ~~as quickly as possible~~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 ~~checked them out or~~ 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 should not be left unattended in automobiles ~~or in view of passers-by~~, for example.

2. Escorting Visitors and Patients. Visitors and patients must be escorted and monitored when on University premises where PHI is located to ensure they do not access PHI. Health Care Components shall not permit unescorted visitors or patients in areas where patients are being treated or that contain PHI.

Persons who are not employed by the Health Care Component, including but not limited to pharmaceutical representatives and servicemen, shall not be in areas in where patients are being seen or treated 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 secured.

4. Equipment. Equipment containing PHI (e.g., desktop computers, medical equipment, fax machines, monitors) must be physically and/or technically secured when not attended, such as by encryption or physical security features (e.g. alarms, locks), as appropriate. University-owned equipment that contains PHI may not be removed from University premises solely for convenience; ~~without~~ supervisor approval for removal is required. 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.

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 AES Encryption standards for H.323 protocol communications. ~~Contact~~ 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 is acceptable (all campuses.) PHI ~~sent should be limited to the minimum necessary and~~ should be sent as a limited data set when possible. The minimum necessary standard (See Privacy–21, The Minimum Necessary Rule) must be observed when applicable.

3. E-mail Between OUHSC.EDU/OU.EDU and HCAHealthcare.com E-mail Addresses. Sending e-mails that contain PHI for Treatment, Payment, or Health Care Operations between ouhsc.edu or ou.edu and HCA Healthcare.com email addresses is secure and therefore acceptable. PHI sent should ~~be limited to the minimum necessary and 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. The use of e-mail to transmit PHI outside the University for Treatment, Payment, or Health Care Operations is prohibited unless the message is encrypted between sender and recipient in a manner that complies with HIPAA. IT Security can advise on whether secure connections exist with a particular recipient. Options include emailing from the EMR, through a secure patient portal, or using **[secure]** in the subject line. Workforce ~~m~~Members may not email PHI off-campus without first obtaining their supervisor's approval. Each Health Care Component shall have in place procedures for emailing PHI. ~~(Contact IT Security for encryption information.)~~

    a. When E-mail Encryption is Available. Subject to the Health Care Component's policies and procedures, University personnel may send PHI via encrypted email.

    b. Without Encryption Capabilities (E-Mail Communication Denial). If a patient sends an e-mail to an employee, student, 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 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."

*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 ~~p~~Personnel shall refer to their Health Care Component email ~~policy or~~ procedure or refer the patient to the supervisor.

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

Confidentiality Notice

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.

6. Electronic Documents. Documents and attachments and/or images containing PHI generally must be stored on network servers with appropriate security restrictions in accordance with IT Security policy, rather than on portable devices or unsecure desktop computers. (~~Contact~~ IT Security ~~for~~ can provide specific information on these servers.)

7. Portable Computing Devices (e.g., laptops and hand-held computers). Employees, volunteers, and students must use extreme caution when using Portable Computing Devices to store PHI. PHI should not be stored on Portable Computing Devices unless absolutely necessary; it should be stored on servers in a secure enterprise data center in accordance with IT Security policy. Portable Computing Devices must never be left unattended in unsecured places.

   Those storing PHI on personal portable devices are responsible for the security of the PHI stored on such devices. If PHI ~~contained~~ is stored on such devices, ~~the~~ the device must be encrypted pursuant to the University Portable Computing Device Security Policy and Standard. All University Standards for Portable Computing Device Security, such as password protection, must be followed. The failure to take appropriate 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 ~~made clear~~ stated that it considers the storing of PHI on unencrypted portable devices to be an act of deliberate indifference with regard to the protection of PHI.

8. Other Uses ~~of the~~ /Internet. Any other electronic transmission of PHI requires that appropriate safeguards and procedures be implemented. Health Care Component~~'~~s should contact ~~the Privacy Official~~ IT Security or the HIPAA Security Officer for more information.

9. ~~Use of~~ 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.

10. ~~Use of~~ 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, imposing these requirements on the vendor during the contracting process or working with IT Security. (See the IT website regarding Electronic Data Disposal and Reuse - http://it.ouhsc.edu/policies/DataDisposal.asp.)

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 Law Enforcement is expected in case of theft.

III. REFERENCES

A. HIPAA Privacy Regulations, 45 CFR §164.530.
B. OUHSC Property Inventory § 581 (B)(2) AND Equipment Inventory Personal Usage Authorization Form.
C. Norman Campus Property Control, Temporary Equipment Use Agreement.

UNIVERSITY OF OKLAHOMA

HIPAA Privacy Policies

Subject: Sanctions	**Page:** 1 of ~~2~~5
Policy #: Privacy-19 (Admin.)	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Last Revised:** ~~04/26/10; 09/14/12; 09/16/13~~February 1, 2016

I. ~~I.~~ PURPOSE

~~To establish a process for imposing sanctions in the event the University's Privacy Policies or the Privacy Regulations are violated.~~

~~II. POLICY*~~

~~The~~ University ~~will apply sanctions as appropriate against~~ Workforce Members (employees, students/trainees, and volunteers) are expected to comply with University ~~Personnel and University~~ HIPAA Privacy and Security policies and procedures, as well as with the related policies and procedures of their department or area. Federal law requires that the University have and apply appropriate, consistent sanctions against Workforce Members and Business Associates who fail to comply with HIPAA or the University's ~~Privacy Policies and/~~or ~~the~~Health Care Component's HIPAA Privacy ~~Regulations.~~ and Security policies and procedures (together, "HIPAA").

The purpose of this policy is to establish sanctions to address HIPAA violations by OU Workforce Members and Business Associates.

II. POLICY*

The University, through its Health Care Components and Human Resources offices, will apply sanctions when appropriate against Workforce Members and University Business Associates who fail to comply with HIPAA.

The University will not impose sanctions against University Personnel or Business Associates for: (~~a~~A) engaging in good faith whistleblower activities related to Privacy issues; (~~b~~B) submitting a complaint in good faith to the Secretary of the Department of Health and Human Services or other enforcement agency; (~~c~~C) participating in an investigation regarding Privacy issues; or (~~d~~D) appropriately registering opposition to a violation of the Privacy Policies or Regulations.

~~II.~~III. ~~III.~~ PROCEDURE

~~A. Employees. A violation of the University's Privacy Policies or Regulations by an employee will also be considered a violation of the University's Compliance and Quality~~

*Capitalized terms are defined in Privacy-01, Definitions

~~Improvement Program (the "Program"). The Program is available on the Office of Compliance website. The sanctions set forth in the Program Corrective Action section apply equally to violations of the University's Privacy Policies. The sanction imposed for a violation of the Privacy Policies depends on the severity of the violation and will be imposed in accordance with the University's Staff or Faculty Handbook, whichever is applicable, and Health Care Component policies.~~

~~B. Students. Students who violate the University's Privacy Policies or Privacy Regulations may be subject to sanctions that may include, but are not limited to, mandatory training, suspension of enrollment privileges, fines, suspension, or expulsion. The type of sanction imposed depends on the severity of the violation. Sanctions will be imposed on students in accordance with applicable University policies and procedures.~~

~~*Capitalized terms are defined in Privacy-01, Definitions~~
~~C. Volunteers. Volunteers who materially violate the University's Privacy Policies or Privacy Regulations will not be permitted to provide further service to the University as a volunteer.~~

~~D. Business Associates. If the University knows of a pattern of activity or practice of a Business Associate that constitutes a material breach or violation of the Business Associate's obligations under the contract with the University or under the Privacy Regulations, the University (through the University Privacy Official and Health Care Components) will take reasonable steps to cure the breach or end the violation, as applicable, and, if such steps are unsuccessful or not appropriate, shall (1) terminate the contract, if feasible; or (2) report the problem to the Secretary of the Department of Health and Human Services or other applicable enforcement agency.~~

~~E. Documentation.~~ Health Care Components shall follow the guidance below in evaluating whether sanctions are appropriate for HIPAA violations and, if so, for implementing those sanctions.

Documentation regarding any sanction imposed for a violation of the Privacy Policies or Privacy Regulations shall be retained in the sanctioned person's personnel or student file, whichever is applicable, in written or electronic format, for at least six (6) years. Copies of such documentation ~~should~~shall be forwarded to the University Privacy Official upon request, who also ~~should~~shall maintain such documentation for ~~the minimum retention period. Documentation of any sanction imposed against a Business Associate should be retained by the University Privacy Official for the minimum retention period.~~ at least six (6) years.

A. ~~F.~~ Sanctions~~. When imposing sanctions for~~ Against Business Associates. If the ~~inappropriate Use and Disclosure of or access to Protected Health Information, consideration should be given to issues such as whether~~ University, through the ~~Use~~Privacy Official, determines that a Business Associate's pattern of activity or practice constitutes a material breach or ~~Disclosure or access was made as a result~~ violation of ~~(1)~~the Business Associate's obligations under HIPAA or under its Business Associate agreement with the University, then the University Privacy Official:

1. Will take or require the Business Associate to take reasonable steps to cure the breach or end the violation, as applicable, or

2. If such steps are unsuccessful or not appropriate or sufficient to protect the University or its PHI, shall (a) terminate the Business Associate Agreement, if feasible; and/or (b) report the problem to the Secretary of the Department of Health and Human Services or other applicable enforcement agency.

B. Sanctions Against University Students/Trainees. If the University, through the Privacy Official or its Health Care Components, determines that a University student or trainee has violated HIPAA, the University, through the appropriate Health Care Component dean or designee and in coordination with the Privacy Official, will impose appropriate sanctions against the student or trainee.

1. Sanctions may include, but are not limited to, additional training, suspension of enrollment privileges, fines, suspension from the program, or expulsion from the college or University.

2. Sanctions will be imposed against students and trainees in accordance with applicable University and college policies and procedures and will take into consideration the trainee status of the student, as well as the University's education mission and any other mitigating factors.

C. Sanctions Against Employees (including Residents and Fellows) If the University, through the Privacy Official and its Health Care Components, determines that a University employee has violated HIPAA, the University, through the appropriate Health Care Component and Human Resources office, shall impose appropriate sanctions against the employee.

1. Managers/unit heads should consult with their Human Resources representative, as appropriate, when considering and implementing sanctions against employees. The applicable Graduate Medical Education Office or Dean's office shall be responsible for sanctions against residents and fellows.

2. When determining what sanction is appropriate, the manager or individual implementing the sanctions shall give consideration to the categories of offenses and to whether mitigating factors exist.

a. Categories of Offenses- It is not possible to anticipate each type of HIPAA violation that may occur, nor is it appropriate to assume one sanction is appropriate for all types of violations in all circumstances. However, consistency is important. The offense categories below provide guidance to Health Care Components on categorizing offenses but are not intended to be all-inclusive or limiting. There may be cases in which a violation does not appear to fit within a particular category or does not appear to be consistent with the violation. In such cases, documentation of the reasons for varying from these guidelines should be retained in the file associated with the violation investigation.

1. **Category 1: Accidental or Inadvertent Violation or Failure to Follow HIPAA Privacy and Security Policies and Procedures.** This category includes unintentional violations of HIPAA that was caused by carelessness ~~or negligence, (~~, lack of training, or human error, as well as violations due to poor job performance or lack of performance improvement. Examples of Category 1 violations include:

- Accessing PHI without a written Authorization that complies with University policy and applicable law;
- directing PHI via mail, e-mail, or fax to the wrong recipient(s)

- giving a clinic visit summary or lab result to the wrong patient
- releasing PHI without proper patient Authorization;
- leaving PHI on an answering machine or discussing PHI in a public area;
- failing to report HIPAA violations the Workforce Member causes, observes, or has knowledge of;
- improperly disposing of PHI;
- failing to properly sign off from or lock computer when leaving a work station unattended;
- failing to properly safeguard password or log-in credentials;
- failing to safeguard a portable device or the PHI on an electronic device from unauthorized access, loss, or theft that led to view by an unauthorized individual accessing PHI;
- transmitting PHI via an unsecured method

~~1.~~2. **Category 2~~):~~ Deliberate or Purposeful HIPAA Violation But Without Harmful Intent.** This category involves an intentional violation due to curiosity~~,~~ or ~~(3) the~~ desire to gain information for personal ~~gain or malice.~~ use. Examples of this type of violation include:

- ~~**IV.**~~Second offense of any Class I offense (does not have to be the same offense);
- Accessing, Using, or Disclosing PHI without a legitimate need to do so, such as an employee checking his own record, reviewing the results of a coworker's lab work, or accessing a family member's or friend's record outside of the employee's job responsibilities;
- posting PHI on a social media or similar act;
- removing PHI from the premises solely for convenience and without proper approval;
- sharing or using shared access codes or log-in credentials;
- failing to cooperate with authorized individuals in the investigation, mitigation, or resolution of a HIPAA incident

3. **Category 3: Willful and Malicious Violation with Harmful Intent.** This category includes an intentional violation causing or likely to cause harm to a patient or the University. Examples of this type of violation include:

- Repeat of any Class I or II offense (does not have to be the same offense);
- Disclosing PHI to an unauthorized individual or entity for illegal or illicit purposes (e.g., identity theft, fraud);
- creating or modifying PHI for unauthorized or improper purposes or under false pretenses;
- Disclosing a patient's PHI to the media;
- obtaining PHI under false pretenses;

b. Sanctions Against Employees by Category. Once the manager or individual imposing the sanction has determined the category of offense, the

sanction(s) imposed should be consistent with the following, unless mitigating factors exist.

1. Category 1 - Sanctions for Category 1 offenses may include, but are not limited to:
   - Termination of employment;
   - Suspension for a stated suspension period, generally one to three days;
   - Retraining on the proper use of HIPAA forms and/or policies and procedures, as appropriate;
   - Written reprimand maintained in employee's personnel file permanently;
   - Informal verbal counseling/reprimand;
   - verbal counseling/reprimand, documented in the investigation file and, if appropriate, the personnel file

2. Category 2– Sanctions for Category 2 Offenses may include, but are not limited to:
   - Termination of employment;
   - Suspension for a stated period, generally one to three days;
   - Retraining on proper use of HIPAA forms and/or policies and procedures, as appropriate;
   - Written reprimand maintained in the investigation file and in the employee's personnel file permanently

3. Category 3 – Sanctions for Category 3 Offenses may include, but are not limited to:
   - Termination of employment/abrogation of tenure;(administered in conformance with the OUHSC Faculty Handbook, including, Section 3.16 "Abrogation of Tenure, Termination of Employment, Severe Sanctions; Summary Suspension; and Other Disciplinary Actions Imposed for Failure to Comply with The University Compliance Program, Professional Practice Plan Billing Compliance Policy, or Other Federal or State Mandates");
   - Extended period of suspension, generally 4 to 5 days

c. Sanctions Against Volunteers. Managers/unit heads may not permit volunteers who violate HIPAA to provide further service to the University as a volunteer in a Health Care Component if the violation is a Category 2 or 3 offense, absent mitigating factors.

VI. MITIGATION FACTORS

Sanctions may be modified based on mitigating factors, resulting in lesser or greater sanctions than those included in this policy. The manager or individual determining the sanction in a particular case should include documentation in the investigation file of what mitigating factors, if any, were taken into consideration when determine the appropriate sanction. Mitigating factors may include but are not limited to:

- Violation of sensitive PHI such as HIV, psychiatric, substance abuse, or genetic data
- High number of people or volume of data affected
- High exposure (e.g., financial, reputational) for the University

- Large University or HCC expense incurred, such as for breach notifications
- Hampering the investigation; lack of truthfulness or cooperation
- Violator's level of training in HIPAA (e.g., inadequate training, training barriers)
- Culture of surrounding environment (e.g., investigation determines inappropriate practices in business unit with manager's knowledge or direction)
- Victim(s) suffered no financial, reputational, or other personal harm and risk of compromise of PHI is low, as determined by a risk assessment
- Violator voluntarily reported the violation in a timely manner and cooperated with the investigation
- Violator showed remorse and accepted responsibility for the violation
- Frequency with which the violator accesses or Uses PHI as part of her job responsibilities
- Violation action was confirmed to have been taken under pressure from an individual in a position of authority
- Time between repeat offenses

V. REFERENCES

~~A.~~ HIPAA Privacy Regulations, 45 ~~C.F. R.~~CFR 164.530(e~~).~~

A.)(1).

UNIVERSITY OF OKLAHOMA

HIPAA Privacy Policies

Subject: Uses and Disclosures - General	**Page:** 1 of 2
Policy #: Privacy-20 (Uses & Disclosures)	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Last Revised:** January 29, 2016

I. PURPOSE

To outline required and permitted Uses and Disclosures of Protected Health Information.

II. POLICY*

The University cannot Use or Disclose Protected Health Information, except as permitted by its Privacy Policies and the Privacy Regulations, summarized below.

A. Required Disclosures

The University will Use or Disclose Protected Health Information: (a) to a patient, when requested under, and as required by Privacy-05, Patient Access to Protected Health Information; and Privacy-06, Accounting of Disclosures; and (b) when required by the Secretary of the Department of Health and Human Services to investigate the University's compliance with the Privacy Regulations or otherwise Required by Law.

B. Permitted Uses and Disclosures

The University and University Personnel are permitted to Use or Disclose Protected Health Information as follows:

(1.) For Treatment, Payment, or Health Care Operations, as permitted by and in compliance with Privacy-22, Treatment, Payment, and Health Care Operations;

(2.) Incident to a Use or Disclosure otherwise permitted or required by the Privacy Regulations (such as to Buisness Associates or Personal Representatives), as long as the Privacy-21, Minimum Necessary (Privacy-21) and Privacy-18, Safeguard Privacy-18 policies have been are followed;

(3.) pPursuant to an Authorization as permitted by Privacy-23, Authorization, and Privacy-28, Marketing;

(4.) Ppursuant to an agreement under, or as otherwise permitted by, Privacy-26, Disclosures
to Family and Others Involved in Patient's Care;, and Privacy-33, Facility Directory; and

(5.) Aas permitted by and in compliance with Privacy-24, Mental Health Records; Privacy-25, Required by Law; Privacy-27, Business Associate; Privacy-29, Fundraising;

*Capitalized terms are defined in Privacy-01, Definitions

Privacy-30, Research; and Privacy-31, Limited Data Set;.

(6.) Tto report unlawful or unprofessional conduct or conduct that endangers others that a whistleblower believes in good faith the University has engaged in, so long as the Disclosure is to a Health Oversight Agency/Public Health Authority or health care accreditation organization that has authority to investigate such conduct or to an attorney retained to advise the reporting party on legal options;.

(7.) bBy University Personnel who is the victim of a crime reporting to Law Enforcement, so long as the PHI disclosed is about the suspect and is limited name and address, date and place of birth, SSN, ABO blood type and rh factor, type of injury, date and time of treatment, date and time of death if applicable, and distinguishing physical characteristics; and.

(8.) Oof certain immunization records without the standard Authorization form to a school about an individual who is a student or prospective student of the school (or to the individual, if the requested information is for presentation to a school) and if:

a. the PHI that is disclosed is limited to proof of state-required immunizations; and

b. the school is required by state or other law to have such proof of immunization prior to admitting the individual; and

c. the University obtains and documents the request for the disclosure from either:

i. a parent, guardian, or other person acting in loco parentis of the individual, if the individual is an unemancipated minor; or

ii. the individual, if the individual is an adult or emancipated minor.

The Health Care Component may accept a verbal request for these immunization records. All verbal requests must be documented in the patient's medical record. Health Care Components may use the Immunization Release Request Form, available on the HIPAA website, or similar documentation.

For other Uses and Disclosures, University Personnel should consult with the Privacy Official or the Office of Legal Counsel.

III. REFERENCES

A. 45 C.F. R. § 164.502.
B. 45 C.F.R. § 164.512.

UNIVERSITY OF OKLAHOMA

HIPAA Privacy Policies

Subject: Minimum Necessary Rule	**Page:** 1 of 3
Policy #: Privacy-21 (Uses & Disclosures)	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Last Revised:** January 29, 2016

I. PURPOSE

To describe the application of the minimum necessary rule to Uses and Disclosures of and requests for Protected Health Information.

II. POLICY*

University Personnel must make reasonable efforts to limit the Use and Disclosure of and requests for Protected Health Information to the minimum that is reasonably necessary 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;
b. Disclosures to the patient or his/her legal representative (See, Privacy-02, Personal Representatives; and Privacy-05, Patient Access to Protected Health Information);
c. Uses or Disclosures made pursuant to an Authorization (See, Privacy-23, Authorization);
d. Disclosures made to the Secretary of the Department of Health and Human Services for compliance and enforcement of the Privacy Regulations (See, Privacy-20, Uses and Disclosures);
e. Uses and Disclosures Required by Law (See, Privacy-25, Required by Law);
f. Uses and Disclosures required for compliance with HIPAA standardized transactions.

Except as provided above, University Personnel may not Use, Disclose, or request an entire medical record, except when the entire medical record is specifically justified by the individual requesting the record as that which is reasonably necessary to accomplish the purpose for the Use, Disclosure, or request. Language such as the following should accompany ~~these~~ requests for entire medical records: Based on my professional judgement, ~~the~~ this request for the entire medical record is consistent with the Minimum Necessary Standard for the (describe) purpose intended.

Each Health Care Component must designate the University Personnel associated with that Health Care Component who need access to Protected Health Information to carry out their duties **and** must designate the level of access needed and the conditions appropriate to such access.

*Capitalized terms are defined in Privacy-01, Definitions

III. PROCEDURE

A. Access

1. Employee and Volunteer Access: The Role-Based Access Worksheet (available on the HIPAA website and from the Human Resources office) must be completed for each employee and volunteer.

A supervisor within t~~T~~he Health Care Component in which the employee or volunteer works will be responsible for completing the Worksheet upon the employee's or volunteer's initial placement into the Health Care Component and, as applicable, when the employee's or volunteer's responsibilities change. A copy of the Worksheet for employees ~~must~~ should also be sent to Human Resources for inclusion in the employee's file. The original ~~is~~ shall be maintained by the Health Care Component. Volunteer forms must be maintained by the Health Care Component utilizing the volunteer.

~~2. The access granted to students must be determined on a case-by-case basis, depending on the educational activity. A student's access must be determined by, and monitored by, each instructor/supervising individual.~~

University Personnel who are directly involved in a patient's Treatment and care (e.g., physicians and nurses) may have access to all of the patient's Protected Health Information.

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 or as permitted by the Privacy Regulations and these Policies. Accessing records of a family member, for example, is a violation of the minimum necessary rule unless the access is necessary for the performance of an assigned job duty.

2. Student Access: The access granted to students must be determined on a case-by-case basis, depending on the educational activity. A student's access must be determined by, and monitored by, the student's instructor/supervising individual.

B. Disclosures

1. Routine Disclosures: Health Care Components should implement standard protocols, when appropriate, to limit the Protected Health Information Disclosed on a routine or recurring basis. Copies of such protocols shall be maintained by each Health Care Component and provided to the Privacy Official upon request.

2. Non-Routine Disclosures: No 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 which 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. When considering making non-routine Disclosures, consideration should be given 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.

University Personnel may rely, if such reliance is reasonable under the circumstances, on a requested Disclosure as the minimum necessary 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(s); or

(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.

C. **Requests**

1. Routine Requests: Health Care Components should implement standard protocols, when appropriate, to limit the Protected Health Information requested on a routine or recurring basis. Copies of such protocols should be maintained by each Health Care Component and provided to the Privacy Official upon request.

2. Non-Routine Requests: Each Health Care Component 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 of a particular request must be submitted to the Office of Legal Counsel or the University Privacy Official. When considering non-routine requests, the following criteria must be considered: (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.

IV. REFERENCES

A. HIPAA Privacy Regulations, 45 CFR 164.502(b).

B. ~~;~~ HIPAA Privacy Regulations, 45 CFR 164.514(d).

UNIVERSITY OF OKLAHOMA

HIPAA Privacy Policies

Subject: Treatment, Payment, and Health Care Operations	**Page:** 1 of 2
Policy #: Privacy-22 (Uses & Disclosures)	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Last Revised:** January 29, 2016

I. PURPOSE

To establish permitted Uses and Disclosures of Protected Health Information for Treatment, Payment, and Health Care Operations, subject to section II E below.

II. POLICY*

A. Health Care Components may Use or Disclose Protected Health Information for their own Treatment, Payment, or Health Care Operations.

B. Health Care Components may also disclose Protected Health Information:

1. for Treatment activities of another Health Care Provider;

2. to another Covered Entity or a Health Care Provider for the Payment activities of the entity that receives the information; and

3. to another Covered Entity for **certain enumerated** Health Care Operations activities of the entity that receives the information, if each entity either has or had a relationship with the patient who is the subject of the Protected Health Information being requested and the information pertains to such relationship.

PHI can be exchanged between two Covered Entities for the following Health Care Operations: (1) conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; (2) population-based activities relating to improving health or reducing health care costs; (3) protocol development, (4) case management and care coordination; (5) contacting Health Care Providers and patients with information about Treatment alternatives; (6) reviewing the competence or qualifications of Health Care Professionals; (7) evaluating practitioner and provider performance; (8) conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as Health Care Providers; (9) training non-health care professionals; and (10) accreditation, certification, licensing, or credentialing activities.

~~B~~C. Health Care Components that participate in an organized health care arrangement may disclose Protected Health Information about an individual to another Covered Entity that participates in the Organized Health Care Arrangement for **any** Health Care Operations activities of the Organized Health Care Arrangement.

*Capitalized terms are defined in Privacy-01, Definitions

D. For Uses and Disclosures of a patient's Protected Health Information other than for Treatment, Payment, and Health Care Operations of a Health Care Component or another Health Care Provider, an Authorization from the patient pursuant to Privacy-23, Authorization, must be obtained unless Disclosure pursuant to another Policy is permitted and/or required. (Health Care Components should Contact the Office of Legal Counsel or the University Privacy Official for assistance.)

E. For Uses and Disclosures of a patient's Psychotherapy Notes, patient Authorization is required, except:

1. for the Use by the originator of the Notes for Treatment;
2. for the Use of Disclosure by the University for its own mental health training prorams;
3. for the Use or Disclosure by the University to defend itself or its employee in a legal action or proceeding brought by the patient; or
4. as Required by Law.

See Privacy -24, Mental Health Records.

A patient Authorization is required for exchanges of PHI between Health Care Components and University departments that have not been designated as Health Care Components, unless the exchange is specifically permitted under the Privacy Regulations.

F. NoteFor: Uses and Disclosures of information related to an enrolled University Student, Ddue to consent requirements under state law and the Federal Education Rights Privacy Act ("FERPA"), which pertains to student records--including student treatment records -- Health Care Components must include language informing currently enrolled OU students that they are consenting to the use of Protected Health Information for Treatment, Payment, and Health Care Operations purposes in the Acknowledgement of Receipt of Notice of Privacy Practices form. **The consent language is included in the Acknowledgement of Receipt of Privacy-04, Notice of Privacy Practices, as well as in the Consent to Use and Disclose Protected Health Information for In-Office Treatment, Payment, and Health Care Operations form.**

III. REFERENCES

A. HIPAA Privacy Regulations, 45 C.F.R. 164.506.
B. FERPA, 20 USC 1232g; 34 C.F.R. Part 99.

UNIVERSITY OF OKLAHOMA

HIPAA Privacy Policies

Subject: Authorization	**Page:** 1 of 3
Policy #: Privacy-23 (Uses & Disclosures)	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Last Revised:** January 29, 2016

I. PURPOSE

To establish Authorization requirements for Uses and Disclosures of Protected Health Information other than for Treatment, Payment, and Health Care Operations.

II. POLICY*

Health Care Components cannot Use or Disclose Protected Health Information for purposes **other** than Treatment, Payment, and Health Care Operations without a valid written Authorization from the patient, except as otherwise permitted by these Policies or law. The Use or Disclosure made must be consistent with the Authorization.

Information released pursuant to Authorization may include alcohol and/or drug abuse records protected under federal and/or state law. Re-disclosure of such alcohol and/or drug abuse records by the recipient is prohibited without specific Authorization, as stated on the Authorization form.

Except as otherwise permitted by the Privacy Regulations, an Authorization is required in order for a Health Care Component to disclose PHI for purposes other than Treatment, Payment, or Health Care Operations and for Use by or Disclosures to departments and areas of the University that are not designated Health Care Components.

Psychotherapy Notes

University Personnel must obtain an Authorization for any Use or Disclosure of Psychotherapy Notes, except in limited circumstances. See, Privacy-24, Mental Health Records.

Fundraising

Health Care Components must obtain an Authorization to Use and Disclose PHI for certain fundraising activities. See Privacy-29, Fundraising.

Sale

Health Care Components must obtain an Authorization for Use or Disclosure of PHI for which the University or a Health Care Component will be paid. The Authorization must state that the Health Care Component or University will receive money for the Disclosure.

*Capitalized terms are defined in Privacy-01, Definitions

Marketing

Health Care Components must obtain an Authorization for any Use or Disclosure of Protected Health Information for marketing, except in certain circumstances. See, Privacy-28, Marketing.

Conditioning of Authorizations

Generally, Health Care Components may not condition the provision of Treatment to a patient on the receipt of an Authorization, except in the context of Research involving Treatment. See, Privacy-30, Research. Health Care Components may not condition the provision of Treatment or Payment for Treatment on the receipt of an Authorization, unless the purpose of the Authorization is to determine payment of a claim.

One exception to the prohibition on conditioning Treatment on the receipt of Authorization relates to Health Care services provided at the request of a third party. For example, Health Care Components can require an Authorization from the individual as a condition to providing the individual with a drug screening test or physical requested by the individual's ~~an~~ employer.

Revocation of Authorizations

Health Care Components must permit patients to revoke their Authorizations, except to the extent the Health Care Component has already taken action in reliance on the Authorization. To revoke an Authorization, a patient must provide written notice to the Health Care Component that received the original Authorization or to the University Privacy Official.

III. PROCEDURES

A. Any individual desiring access to or a copy of his PHI maintained in a Designated Record Set must submit a valid Authorization to the Health Care Component or University Privacy Official. The Authorization must be in plain language and must contain all of the core elements required by the Privacy Regulations and State law, including the patient's or the patient's Personal Representative's signature. The ~~(See~~ Request for Individual's Health Information/Authorization form is available on the HIPAA website.~~)~~

B. Prior to Using or Disclosing Protected Health Information pursuant to an Authorization, University Personnel must review the Authorization to determine if it is valid. Health Care Components may contact the Office of Legal Counsel or the University Privacy Official for help in determining whether an Authorization is valid. An Authorization is not valid if it contains any of the following defects:

1. the expiration date has passed or the expiration event is known to have occurred;
2. the Authorization has not been filled out completely;
3. University Personnel have knowledge that the Authorization has been revoked;
4. University Personnel have knowledge that some material information in the Authorization is false;
5. the Authorization was obtained by improperly conditioning Treatment upon its

receipt;

6. the Authorization is missing one of the elements required by the Privacy Regulations or State law; ~~or~~
7. if the Authorization is for Psychotherapy Notes, it is combined with another type of Authorization or document; or.
8. the Authorization is combined with another document, resulting in a compound authorization that is for purposes other than Research.

C. If a Health Care Component seeks an Authorization from a patient for a Use or Disclosure of Protected Health Information, the Health Care Component must provide the patient with a copy of the signed Authorization.

D. Health Care Components must keep copies of Authorizations in the patient file for at least six (6) years.

IV. REFERENCES

A. HIPAA Privacy Regulations, 45 C.F.R. 164.508.

UNIVERSITY OF OKLAHOMA

HIPAA Privacy Policies

Subject: Mental Health Records and Psychotherapy Notes	**Page:** 1 of 2
Policy #: Privacy-24 (Uses & Disclosures)	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Last Revised:** January 29, 2016

I. PURPOSE

To establish permitted Uses and Disclosures of mental health records, including Psychotherapy Notes.

II. POLICY*

A. Mental Health Records – General

A patient generally has the right to access his/her mental health records **other than Psychotherapy Notes**. (See the definition of Psychotherapy Notes in Privacy-01Definitions.) A patient can be denied access to his/her mental health records for one of the reasons set forth in Privacy-05, Patient Access to Protected Health Information.

Remember: Psychotherapy Notes have a very limited definition. They are notes recorded (in any medium) by a Health Care Provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record.

Mental health records, other than Psychotherapy Notes, may be Used and Disclosed by University Personnel for Treatment, Payment, and Health Care Operations to the same extent and subject to the same limitations applicable to other types of Protected Health Information, as set forth in these Policies and in accordance with applicable mental health statutes.

Persons or entities who desire access to a patient's mental health records for purposes other than Treatment, Payment, or Health Care Operations must obtain an Authorization as required by Privacy-23, Authorization, unless otherwise permitted by these Policies. The Office of Legal Counsel or the Privacy Official should be contacted for assistance with responding to mental health record requests.

An Authorization for the Use or Disclosure of Psychotherapy Notes cannot be combined with an Authorization for release of other medical records.

B. Psychotherapy Notes

A patient does not have ~~a~~ the right to access Psychotherapy Notes relating to him/herself unless (i) the patient's Treatment professional approves such access in writing; or (ii) the patient obtains a court order authorizing such access.

A patient Authorization must be obtained for **any** Use or Disclosure of Psychotherapy Notes, except for the following purposes:

1. Use by the originator (the creator) of the Psychotherapy Notes for Treatment purposes;

2. Use or Disclosure of Psychotherapy Notes by University Personnel for conducting University-related training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling.~~:~~ The minimum necessary standard should be observed;

3. Use or Disclosure to the Office of Legal Counsel or designee to defend the University or University Personnel in a legal action or other proceeding brought by the patient against the University or an employee of the University;

4. Use or Disclosure to the Secretary of Health and Human Services, or any other officer or employee of the Department of Health and Human Services to whom the authority has been delegated, to conduct enforcement activities;

5. Use or Disclosure needed for oversight of University Personnel who created the Psychotherapy Notes;

6. Use or Disclosure needed by a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or conducting other duties as authorized by law~~; or~~ (See Privacy-25, Required by Law, Disclosures to Coroners/Medical Examiners); or

7. When University Personnel, in good faith, believe the Use or Disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public.

The Privacy Regulations do not permit a H~~h~~ealth P~~p~~lan to condition enrollment, eligibility for benefits, or payment of a claim on obtaining a patient's Authorization to Use or Disclose Psychotherapy Notes.

III. REFERENCES

A. HIPAA Privacy Regulations, 45 CFR § 164.508(a)(3)(2) ~~and § 164.524(a).~~
B. HIPAA Privacy Regulations, 45 CFR §164.524(a).
C~~B~~. 43A Okla. Stat. §1-109.

UNIVERSITY OF OKLAHOMA

HIPAA Privacy Policies

Subject: Required by Law	**Page:** Page 1 of 12
Policy #: Privacy-25 (Uses & Disclosures)	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Last Revised:** January 29, 2016

I. PURPOSE

To set forth requirements pertaining to Uses and Disclosures of Protected Health Information Required by Law.

II. POLICY*

University Personnel may Disclose Protected Health Information without the patient's consent, Authorization, or opportunity to agree or object as required by applicable state and federal laws, including those listed below.

Questions regarding whether a particular Use or Disclosure is Required by Law should be submitted to the ~~Privacy Official or~~ Office of Legal Counsel or University Privacy Official.

A. Abuse or Neglect of Children ~~H. Health Oversight~~
~~B.~~ Adult Victims of Abuse, Exploitation, ~~I. Medicaid~~
B. or Criminally-Injurious Conduct
C. Coroners/Medical Examiners ~~J.~~
D. Death Reports
E. Funeral Directors
~~C.~~F. Government Functions - Specialized
~~D.~~G. Health Oversight

~~E.~~A. ~~Death Reports~~
~~F.~~H. Judicial and Administrative Procedure ~~K. Coroners/Medical Examiners~~

1. Court Orders ~~L. Funeral Directors~~
2. Subpoenas ~~M. Organ and Tissue Donations~~

~~G.~~I. Law Enforcement ~~N. Worker's Compensation~~
J. Medicaid Program
K. Organ and Tissue Donations
~~H.~~L. Public Health ~~(including:)~~Activities
~~I.~~M. Threats to Health and Safety
~~1.~~ Worker's Compensation~~Statistical Reports~~
~~2. Birth Certificates~~
~~3. Death Certificates~~
~~4. Communicable Diseases~~
N.

III. PROCEDURE

A. Abuse or Neglect of Children.

1. Reporting Child Abuse, Neglect, or the Birth of a Chemically-Dependent Child. University Personnel who have reason to believe that a child under the age of 18 is a

victim of abuse or neglect or who attend the birth of a child who tests positive for alcohol or a controlled dangerous substance are required by state law to promptly notify the

~~*Capitalized terms are defined in Privacy-01, Definitions~~

Oklahoma Department of Human Services. Health Care Components should establish procedures for facilitating and coordinating reporting requirements. No patient Authorization is required for this Disclosure, which shall be logged in the Accounting of Disclosure Log.

a. "Abuse" for purposes of this section means harm or threatened harm to the child's health, safety, or welfare by a parent; legal guardian; custodian; foster parent; adult residing in the home of the child; the owner, operator, or employee of a child care facility; or an agent or employee of a private residential home, institution, facility, or day treatment program.

b. "Neglect" for purposes of this section means (i) failure to provide adequate food, clothing, shelter, medical care, and supervision; (ii) failure to provide special care which is necessary because of the physical or mental condition of the child; or (iii) abandonment.

c. Reports of abuse or neglect shall be made to the telephone hotline established by DHS, in accordance with state law. A written record of each such report and the circumstances surrounding such report shall be maintained by the Health Care Component making the report. The report must contain the following:

- The names and addresses of the child and the child's parents or other persons responsible for the child's health, safety, or welfare;
- The child's age;
- The nature and extent of the abuse or neglect, including any evidence of previous injuries;
- Whether the child has tested positive for alcohol or a controlled dangerous substance; and
- Any other information that may be helpful in establishing the cause of the injuries and the identity of the person or persons responsible.

d. Health Care Components also must provide copies of the results of the examination or copies of the examination on which the report was based and any other clinical notes, x-rays, photographs, and other previous or current records relevant to the case to DHS and Law Enforcement officers conducting a criminal investigation into the case and to employees of the Department of Human Services conducting an investigation of alleged abuse or neglect in the case, *upon written verification* by the applicable agency of a pending investigation.

Verification forms for DHS and Law Enforcement are available on the University HIPAA forms page and from the University Privacy Official.

2. Reporting Criminally Inflicted Injuries. University Personnel examining, attending, or treating a child suffering from what appears to be criminally injurious conduct, including, but not limited to, a misdemeanor or felony that results in bodily injury, threat of bodily injury, death, or child physical or sexual abuse shall promptly report the matter to the local police department. The report may require the disclosure of Protected Health Information relevant to the investigation. Health Care Components should establish procedures for facilitating and coordinating reporting requirements.

3. Notification. To the extent a report is made ~~pursuant to 1 (a) or (b)~~as described above, University Personnel must promptly notify the Personal Representative of the child who is the subject of the report, unless University Personnel, in the exercise of professional judgment, believe informing the Personal Representative would place him/her at risk of serious harm or if they believe such Personal Representative is responsible for the abuse, neglect, or other injury and that informing such person would not be in the best interests of the child.

B. Adult Victims of Abuse, Neglect, Exploitation, or Criminally-Injurious Conduct.

1. Reporting Abuse, Neglect, and Domestic Violence. University Personnel who have reasonable cause to believe that a Vulnerable Adult is suffering from abuse, neglect, or exploitation shall promptly report the matter to the Oklahoma Department of Human Services; the office of the district attorney in the county in which the suspected abuse, neglect, or exploitation occurred; or the local police or sheriff's department, in accordance with state law.

a. A "Vulnerable Adult" is a patient who is incapacitated or who, because of physical or mental disability, incapacity, or other disability, is substantially impaired in the ability to provide adequately for the care or custody of him/herself; is unable to manage his or her property and financial affairs effectively; is unable to meet essential requirements for mental or physical health or safety; or is unable to protect him/herself from abuse, neglect, or exploitation without assistance from others.

b. "Abuse" for purposes of this section means causing or permitting: (i) the infliction of physical pain, injury, sexual abuse, sexual exploitation, unreasonable restraint or confinement, or mental anguish, or (ii) the deprivation of nutrition, clothing, shelter, health care, or other care or services without which serious physical or mental injury is likely to occur to a Vulnerable Adult by a caretaker or other person providing services to a Vulnerable Adult.

c. "Exploitation" or "Exploit" means an unjust or improper use of the resources of a Vulnerable Adult for the profit or advantage, economic or otherwise, of a person other than the Vulnerable Adult through the use of undue influence, coercion, harassment, duress, deception, false presentation, or false pretense.

d. "Neglect" for purposes of this section means: (i) the failure to provide protection for a Vulnerable Adult who is unable to protect his or her own interest; (ii) the failure to provide a Vulnerable Adult with adequate shelter, nutrition, health care, or clothing; or

(iii) the causing or permitting of harm or the risk of harm to a Vulnerable Adult through the action, inaction, or lack of supervision by a caretaker providing direct services.

e. Reports of victims of Abuse, Neglect, or Exploitation must contain the name and address of the Vulnerable Adult, the name and address of the caretaker, if any, and a description of the current location and current condition of the Vulnerable Adult and of the situation which may constitute Abuse, Neglect, or Exploitation of the Vulnerable Adult, in accordance with state law. Health Care Components shall provide PHI to Law Enforcement officers or ~~employees~~authorized public officials conducting investigations *upon written verification* by the applicable agency of a pending investigation.

f. Verification forms for DHS and Law Enforcement are available on the University HIPAA forms page and from the University Privacy Official.

2. Reporting Criminally-Injurious Conduct. Any University Personnel examining, attending, or treating an adult patient for what appears to be criminally-injurious conduct, including, but not limited to, a misdemeanor or felony that results in bodily injury, threat of bodily injury, or death, shall promptly report the matter to the local police department. The report may require the disclosure of Protected Health Information relevant to the investigation. Health Care Components should establish procedures for facilitating and coordinating reporting requirements.

3. Notification. To the extent a report is made ~~pursuant to 2 (a) or (b)~~as described above, University Personnel must promptly notify the patient or the Personal Representative of the Vulnerable Adult who is the subject of the report, unless University Personnel, in the exercise of professional judgment, believe informing the ~~individual~~patient or the Personal Representative would place him/her at risk of serious harm of if they believe that such Personal Representative is responsible for the abuse, neglect, or other injury, and that informing ~~such person~~the Personal Representative would not be in the best interests of the Vulnerable Adult.

C. Coroners and Medical Examiners. The University may Disclose Protected Health Information to coroners and medical examiners as necessary for the purpose of their identifying a deceased person, determining a cause of death, or carrying out their duties as authorized by law. To the extent necessary, such Protected Health Information may be Disclosed prior to, and in reasonable anticipation of, the patient's death. A *written request* from the coroner or medical examiner that includes the basis of the request must be obtained prior to the release.

D. Deaths on University Property. Certain deaths of patients occurring on University property must be reported by University Personnel to the President of the University, or his or her designee, as well as to Law Enforcement. The President or his or her designee will notify the Executive Dean of the College of Medicine, who must promptly report the death to the Office of the Chief Medical Examiner prior to release of the body. Types of deaths subject to investigation that should be reported include violent deaths; suspicious deaths; deaths related to disease that might constitute a threat to public health; deaths unattended by a physician for a fatal or potentially fatal illness; a death after an unexplained coma; deaths that are medically unexpected and that occur in the course of a therapeutic procedure; a death of an inmate; and deaths of persons who will be cremated, buried at sea, transported out of state, or otherwise made unavailable for pathological study. Within thirty-six (36) hours of death, a written report must be submitted to the Office of the Chief Medical Examiner, which must be accompanied by true and correct copies of all medical records of the University concerning the deceased patient.

The Chief Medical Examiner may require the University to produce the patient's Protected Health Information including records, documents, or other items regarding the deceased patient that are necessary to investigate the death. The requested Protected Health Information may be Disclosed without the Authorization of the patient's Personal Representative. However, the University must limit disclosure of such Protected Health Information to that which is specifically requested *in writing* by the Chief Medical Examiner.

E. Funeral Directors. The University may Disclose Protected Health Information to funeral directors as necessary for them to carry out their duties with respect to the decedent. To the extent necessary, such Protected Health Information may be Disclosed prior to, and in reasonable anticipation of, the patient's death. A *written request* from the funeral director that includes the basis of the request must be obtained prior to the release.

F. Government Functions - Specialized.

1. Military. The University may Use and Disclose Protected Health Information of patients in the United States and foreign armed forced for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission~~.~~, subject to certain requirements. The Office of Legal Counsel or University Privacy Official should be consulted to confirm that the requirements of such Use or Disclosure are met.

2. National Security~~.~~ and Related Services. The University may Disclose Protected Health Information to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act, and to protect the President of the United States and certain other public officials as authorized by law. The Office of Legal Counsel or University Privacy Official should be consulted to confirm that the requirements of this Disclosure are met.

3. Correctional Institutes/Inmates. The University may Disclose to a Correctional Institution or Law Enforcement Official having lawful custody of an inmate or other individual, and the Correctional Institution or Law Enforcement Official may use Protected Health Information about such individual, if the Correctional Institution or such Law Enforcement Official represents that such Protected Health Information is necessary for: (~~i~~a) the provision of Health Care to such individuals; (~~ii~~b) the health and safety of such individual or other inmates; (~~iii~~c) the health and safety of the officers or employees of or others at the Correctional Institution or other persons responsible for the transporting of inmates; (~~iv~~d) Law Enforcement on the premises of the Correctional Institution; and/or (~~v~~e) the administration and maintenance of the safety, security, and good order of the Correctional Institution. The Office of Legal Counsel or University Privacy Official should be consulted to confirm that the requirements of this Disclosure are met.

~~C~~

G. Health Oversight Activities. University personnel may disclose PHI to a Health Oversight Agency for certain oversight activities authorized by law, upon receipt of a written request for such. The request must state the purpose for which the PHI is sought. The Office of Legal Counsel or the University Privacy Official must be consulted prior to any release of PHI under this section.

H. Judicial and Administration Procedure – PHI may be released pursuant to:

1. Court Orders./Administrative Orders. A court order is a direction of the court that orders a party to produce certain specified documents. An administrative order is issued by an administrative tribunal. Upon the receipt of a court order for the Disclosure of medical records containing Protected Health Information, University Personnel or the recipient of the order must immediately forward the court order to the University's Office of Legal Counsel or designee. Upon determining that the court order is valid and meets all legal requirements, the University Personnel will be advised to release the information pursuant to the court order. The patient whose records are being requested is not required to provide an Authorization for the Disclosure of the records pursuant to a court order.

a. Special Requirements for Court Orders Relating to Substance Abuse Records. Records of the identity, diagnosis, prognosis, or Treatment of University patients maintained in connection with substance abuse education, prevention, training, treatment, rehabilitation, or Research conducted, regulated by, or assisted by any United States department or agency shall be confidential, in accordance with State law and *may not be released under a court order* unless the court order complies with 42 C.F.R 2.13(a) and 2.61-2.67.

b. Disclosure of Substance Abuse Records. The content of these records may be Disclosed to third parties as follows: (i) in accordance with the patient's prior written Authorization; (ii) to medical personnel to the extent necessary to meet a bona fide medical emergency; (iii) to qualified personnel for the purpose of conducting scientific Research, management audits, financial audits, or program evaluation only if the patient is not identified directly or indirectly; (iv) upon receipt of a valid court order that meets all of the requirements of 42 C.F.R. 2.113 (a) and 2.61-2.67.

2. Subpoenas/Discovery Requests. A subpoena is a unilateral request of a party for the production of documents. A subpoena is not generally approved by a judge. Therefore, it is important for the University to determine whether the patient's Authorization or a court order is required for the release. **All subpoenas must be sent to the Office of Legal Counsel or designee for this determination.**

a. The subpoena must be accompanied by Satisfactory Assurance that reasonable efforts were made to notify the patient of the request (this may be in the form of proof that the individual has gotten notice of the request for his/her PHI) or to obtain a qualified protective order.

b. The satisfactory assurance of notice must include, at a minimum, a written statement and supporting documentation that: (i) good faith effort was made to provide written notice to the patient; (ii) the notice included sufficient information about the proceeding such that the patient could object, and (iii) the time to raise objections has passed and none were filed or, if filed, have been resolved.

c. The satisfactory assurance for a qualifying protctive order must include, at a minimum, a written statement and supporting documentation that: (i) the parties agreed to a protective order and have presented it to a court or administrative tribunal with jurisdiction over the matter, or (ii) a qualifying protective order has been requested.

Upon receipt of a subpoena, the recipient of the subpoena must immediately forward the subpoena to the Office of the Office of Legal Counsel or its designee for a determination of whether PHI can be released pursuant to the subpoena.

~~D. Disclosures for~~ I. Law Enforcement ~~Purposes~~Disclosures.

1. Locate or Identify an Individual. Certain limited Protected Health Information regarding a patient may be Disclosed to a Law Enforcement Official who requests such information to identify or locate a suspect, fugitive, material witness, or missing person. Absent a request, such information may not be Disclosed. A request may be made orally or in writing and may include a general request seeking the public's assistance in identifying a suspect, fugitive, material witness, or missing person. The individual making the request must be asked to sign the Verification form located on the HIPAA forms page.

a. If a request is made by a Law Enforcement Official--including OU Campus Police--for a patient's Protected Health Information, the Office of Legal Counsel shall be contacted immediately to authenticate the request for Disclosure and to determine whether the official is authorized to make such a request. Upon determining that the request is valid, the Office of Legal Counsel shall direct the appropriate person(s) to provide the limited information set forth below.

b. The Disclosure of Protected Health Information pursuant to this section is limited to the following:

- Name and address
- Date and place of birth
- Social Security Number
- ABO, blood type, and rh factor
- Type of injury, if applicable
- Date and time of treatment
- Date and time of death, if applicable
- A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair, scars, and tattoos.

University Personnel ~~should~~ may not disclose any of the following information: DNA data and analyses, dental records, or typing samples or analyses of tissues or bodily fluids other than blood.

2. Administrative Requests. The University may disclose Protected Health Information to Law Enforcement Officials pursuant to an administrative request (including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized by Federal or State law), so long as (i) the information sought is relevant and material to a legitimate Law Enforcement inquiry; (ii) the request is specific and limited in scope to the extent reasonably practicable for the purpose; and (iii) the de-identified information cannot reasonably be used. University Personnel should consult with the Office of Legal Counsel or University Privacy Official before making any Disclosures pursuant to this provision.

3. Patient Crime Victim. In addition to other Disclosures regarding potential victims of a crime, the University may disclose to Law Enforcement Officials information about a patient who is or is suspected to be a victim of a crime, if (i) the patient consents to the Disclosure; or (ii) if the patient is unable to provide consent~~,~~ due to incapacity or emergency, if all of the following requirements are met: (a) the Law Enforcement Official represents~~—preferably~~ via a Verification form or similar~~—~~ ~~—~~(a) that such information is needed to determine whether a violation of law by a person other than the patient has occurred, that such information is not intended to be used against the patient, ~~and~~(b) that immediate Law Enforcement activity that depends on the Disclosure would be materially and adversely affected by waiting until the patient is able to consent; and (~~b~~c) that the Disclosure is in the best interest of the patient, as determined by University Personnel in the exercise of professional judgment.

Verification forms for ~~(ii) (a) above~~Law Enforcement to sign are available on the University's HIPAA forms page and from the University Privacy Official. University Personnel should consult with the Office of Legal Counsel or University Privacy Official before making any Disclosures pursuant to this provision.

4. Crime on Premises. The University may Disclose to Law Enforcement Officials PHI that University Personnel believe in good faith constitutes evidence of criminal conduct that occurred on University ~~property~~premises. University Personnel should consult with the Office of Legal Counsel or University Privacy Official before making any Disclosures pursuant to this provision.

5. Off-Premises Emergency. University Personnel providing emergency health care in response to a medical emergency, other than an emergency on University ~~property~~premises, may Disclose PHI to a Law Enforcement Official if the Disclosure appears necessary to alert Law Enforcement to: (i) the commission and nature of a crime; (ii) the location of such crime or that of the victim(s) of such crime; and (iii) the identity, description, and location of the perpetrator of such crime. University Personnel should consult with the Office of Legal Counsel or University Privacy Official before making any Disclosures pursuant to this provision. (This provision is superceded by IIA and IIB above, when applicable.)

J. Medicaid Program. University Personnel must provide the Attorney General of the State of Oklahoma access to all records of Medicaid recipients under the Oklahoma Medicaid Program that are held by University Personnel, for the purpose of investigating the crime of Medicaid fraud or for use or potential use in any legal, administrative, or judicial proceeding, upon receipt of a written request for such. The request must indicate the purpose for which the records are sought. The Office of Legal Counsel or the University Privacy Official should be consulted prior to release.

University Personnel may not refuse to provide the Oklahoma Health Care Authority or the Oklahoma Attorney General with access to such records on the basis that release would violate the patient's right of privacy, privilege against Disclosure or Use, or any professional or other privilege or right. The Disclosure of Protected Health Information pursuant to this Section will not subject any physician or other health services provider to liability for breach of any confidential relationship between a patient and a provider.

~~F. Uses and Disclosures for~~ K. ~~Cadaveric~~ Organ, ~~Eye or~~ and Tissue Donations. University Personnel may Disclose without Authorization Protected Health Information to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric

organs, eyes, or tissue for the purpose of facilitating organ, eye, or tissue donation and transplantation. A *written request* from the organ procurement organization that includes the basis of the request must be received prior to the release.

~~G~~L. Public Health Activities. University Personnel may Disclose Protected Health Information without the written Authorization of the patient to (1) the appropriate ~~state or federal~~public health authority authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability~~;~~ (including birth and death); to conduct public health surveillance, public health investigations, or public health interventions; or, at the direction of a Public Health Authority, to certain foreign governments; (2) to a ~~Public Health Authority~~public health authority authorized by law to receive reports of child abuse or neglect; (3) to certain persons subject to FDA jurisdiction for limited purposes; (4) to persons who may have been exposed to a communicable disease or may be at risk of such, if authorized by law to provide such notice; and (5) to employers for certain medical surveillance work. Any such Disclosures ~~shall~~should be made only after consultation with the Office of Legal Counsel or the University Privacy Official. Such permitted Disclosures shall also specifically include the following:

1. Statistical Reports. The State Department of Health is charged with tracking Health Information within the State of Oklahoma. The Department may request University Personnel to provide to the Division of Health Care Information ("DHCI") certain Health Care information for the purpose of statistical and other similar reports. The University may Disclose the requested information without the patient's written Authorization~~.~~ and must log the Disclosure in the Accounting of Disclosures log. This includes discharge data including, but not limited to, complete discharge data sets or comparable information for each patient discharged.

The Office of Legal Counsel or the University Privacy Official ~~must~~should be notified upon the receipt of a request from the State Department of Health for such information to ensure appropriate reporting. The release of information must be limited to that information that is specified in the request.

2. Birth Certificates. If a birth occurs in a University facility, a birth certificate must be prepared and filed by one of the following University Personnel in the indicated order of priority:

- The physician in attendance at or immediately after the birth; or
- Any other person in attendance at or immediately after the birth.

University Personnel must obtain the personal data, prepare the certificate, secure the signatures required by the certificate, and file the certificate with the local registrar. The physician in attendance must certify to the facts of birth and provide the medical information required by the certificate within five (5) days after the birth. No patient Authorization is necessary to disclose the information used to prepare and file the birth certificate~~.~~; the Disclosure shall be logged in the Accounting of Disclosure log.

3. Death Certificates. A death certificate for a death that occurs in Oklahoma must be filed with the local registrar of the district in which the death occurred, within three (3) days after the death and prior to burial or removal of the body. A funeral director or similar person is responsible for filing the death certificate. However, the funeral director must complete the certificate of death as to personal data and deliver the certificate, within twenty-four (24) hours

after the death, to the attending physician at the University who was responsible for the patient's care or to the medical examiner. The University Personnel responsible for the patient's care or the medical examiner must then complete and sign the certificate of death within forty-eight (48) hours after death. If the University Personnel in charge of the patient's care is not in attendance at the time of the death, the medical certificate must be completed and signed within forty-eight (48) hours after death by other University Personnel in attendance at the time of death. In this instance, the alternate physician must note on the face of the certificate the name of the attending physician and that the information shown is only as reported.

The Authorization of the patient's Personal Representative is not required to disclose information necessary to complete the certificate of death for filing~~.~~; the Disclosure shall be logged in the Accounting of Disclosure log.

4. Communicable or Venereal/Sexually Transmitted Diseases. The term "communicable disease" means an illness due to a specific infectious agent or its toxic products, arising through transmission of that agent or its products from reservoir to susceptible host, either directly as from an infected person or animal, or indirectly through the agent of an intermediate plant or animal host, a vector, or the inanimate environment. It also means an infestation by an ectoparasite and similar species.

The term "venereal disease" or "sexually transmitted disease" means syphilis, gonorrhea, chancroid, granuloma inguinale, lymphogranuloma venereum, and any other disease that may be transmitted from any person to any other person through or by means of sexual intercourse and found and declared by medical science or accredited schools of medicine to be infectious or contagious, and declared to be communicable and dangerous to the public health.

Protected Health Information relating to communicable or venereal/sexually transmitted disease may be released without patient Authorization (and logged in the Accounting of Disclosure log) under the following limited circumstances, following consultation with University Legal Counsel or the University Privacy Official:

a. Court Order. Release of Protected Health Information may be made upon receipt of a valid court order.

b. Administrative Orders. Release of limited Protected Health Information relating to venereal/sexually transmitted or communicable diseases may be made to the State Department of Health *upon the issuance of a final agency order* (an administrative order) issued by an administrative law judge, which is the final order of the State Department of Health, after the administrative law judge determines release is necessary to protect the health and well-being of the general public. In this instance, only the patient's initials shall be Disclosed unless the order specifies the release of the name of the patient.

c. University Personnel Exposures. Release is made of medical or epidemiological information to University Personnel who have had risk exposure. Risk exposure is exposure that is epidemiologically demonstrated to have the potential for transmitting a communicable disease.

d. Statistical Disclosures. Release is made of specific medical or epidemiological information for statistical purposes in such a way that no person can be identified. See, Privacy-32, De-Identified Information.

e. Diagnosis and Treatment. Release is made of Protected Health Information among University Personnel within the continuum of care for the purpose of diagnosis and Treatment of a communicable or ~~venerable~~venereal/sexually transmitted disease of the patient whose information is released.

f. Reports of Venereal/Sexually Transmitted Disease. All University Personnel who make a diagnosis or treat a patient for any venereal/sexually transmitted disease, as defined above, must promptly report the case, in writing, to the State Commissioner of Health. If University Personnel know or have good reason to suspect that the patient with a venereal/sexually transmitted disease is conducting him/herself as to expose other persons to infection, or is about to so conduct him or herself in such a way, University Personnel must notify the State Commissioner of Health of the name and address of the diseased patient and the essential facts of the case. This information may contain the patient's Protected Health Information.

5. Newborn Hearing Tests. Every infant born in Oklahoma must be screened for the detection of congenital or acquired hearing loss prior to discharge from the facility where the infant was born. If the infant requires emergency transfer to another facility for neonatal care, the screening procedure may be administered by the receiving facility prior to discharge of the infant. The results of the screening procedures must be reported to the State Department of Health, in accordance with state law.

6. Birth Defects. The Commissioner of Health may require the University to maintain a list of patients up to six (6) years of age who have been diagnosed with birth defects incorporated within the ~~ICD-9-CM~~published diagnostic code categories 740.0 through 759.9 or such other information as the Commissioner deems appropriate, and all women discharged with a diagnosis of stillbirth or miscarriage. The list shall be made available to the Commissioner upon written request, following consultation with the Office of Legal Counsel or the University Privacy Official. No patient Authorization is required for the Disclsure; the Disclosure shall be logged in the Accounting of Disclosure log.

7. Tumor Registry. The State Commissioner of Health may establish a tumor registry to ensure an accurate and continuing source of data concerning cancerous, precancerous, and tumorous diseases. The tumor registry may include data necessary for epidemiological surveys and scientific research and other data that is necessary to further the recognition, prevention, control, treatment, and cure of cancer and precancerous and tumorous diseases.

The Commissioner may require the University, via statute or written order, to report the following information regarding cancerous and precancerous and tumorous diseases:

a. The patient's name, address, age, race, sex, Social Security ~~Number~~number, and hospital identifier or other identifier;
b. The patient's residential, family, environmental, occupational, and medical histories; and

c. The physician's name~~,~~; diagnosis, stage of the disease, ~~and~~ method of treatment; and the name and address of any facility providing treatment.

~~H. Health Oversight Activities. University personnel may disclose PHI to a Health Oversight Agency for certain oversight activities authorized by law, upon receipt of a written request for such. The request must state the purpose for which the PHI is sought. The Office of Legal Counsel or the University Privacy Official must be consulted prior to any release of PHI under this section.~~

~~I. Medicaid Program. University Personnel must provide the Attorney General of the State of Oklahoma access to all records of Medicaid recipients under the Oklahoma Medicaid Program that are held by University Personnel, for the purpose of investigating the crime of Medicaid fraud or for use or potential use in any legal, administrative, or judicial proceeding, upon receipt of a written request for such. The request must indicate the purpose for which the records are sought. The Office of Legal Counsel or the University Privacy Official should be consulted prior to release.~~

~~University Personnel may not refuse to provide the Oklahoma Health Care Authority or the Oklahoma Attorney General with access to such records on the basis that release would violate the patient's right of privacy, privilege against Disclosure or Use, or any professional or other privilege or right. The Disclosure of Protected Health Information pursuant to this Section will not subject any physician or other health services provider to liability for breach of any confidential relationship between a patient and a provider.~~

~~J. Reports of Certain Deaths. Certain deaths of patients occurring on University property must be reported by University Personnel to the President of the University, or his or her designee, as well as to Law Enforcement. The President or his or her designee will notify the Executive Dean of the College of Medicine, who must promptly report the death to the Office of the Chief Medical Examiner prior to release of the body. Types of deaths subject to investigation that should be reported include violent deaths; suspicious deaths; deaths related to disease that might constitute a threat to public health; deaths unattended by a physician for a fatal or potentially fatal illness; a death after an unexplained coma; deaths that are medically unexpected and that occur in the course of a therapeutic procedure; a death of an inmate; and deaths of persons who will be cremated, buried at sea, transported out of state, or otherwise made unavailable for pathological study. Within thirty-six (36) hours of death, a written report must be submitted to the Office of the Chief Medical Examiner, which must be accompanied by true and correct copies of all medical records of the University concerning the deceased patient.~~

~~The Chief Medical Examiner may require the University to produce the patient's Protected Health Information including records, documents, or other items regarding the deceased patient that are necessary to investigate the death. The requested Protected Health Information may be Disclosed without the Authorization of the patient's Personal Representative. However, the University must limit disclosure of such Protected Health Information to that which is specifically requested by the Chief Medical Examiner.~~

~~K. Disclosures to Coroners and Medical Examiners. The University may Disclose Protected Health Information to coroners and medical examiners as necessary for the purpose of their identifying a deceased person, determining a cause of death, or carrying out their duties as authorized by law. To the extent necessary, such Protected Health Information may be Disclosed prior to, and in reasonable anticipation of, the patient's death. A *written request* from the coroner or medical examiner that includes the basis of the request must be obtained prior to the release.~~

~~L. Disclosure to Funeral Directors. The University may Disclose Protected Health Information to funeral directors as necessary for them to carry out their duties with respect to the decedent. To the extent necessary, such Protected Health Information may be Disclosed prior to, and in reasonable anticipation of, the patient's death. A *written request* from the funeral director that includes the basis of the request must be obtained prior to the release.~~

M. ~~E. Uses or Disclosures to Avert~~ Threats to Health and Safety. University Personnel may, consistent with applicable law and ethical standards, Use or Disclose Protected Health Information if University Personnel, in good faith, believe such Use and Disclosure (i) is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public and the Disclosure is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat; or (ii) is necessary for Law Enforcement Officials to identify or apprehend an individual who (a) has made a statement admitting participation in a violent crime that University Personnel reasonably believes may have caused serious physical harm to the victim (provided that no Disclosure may be made under this circumstance if the Disclosure is made during the course of Treatment to affect the propensity to commit the criminal conduct that is the basis for the Disclosure, or actual counseling or therapy, or if the Disclosure is made during a request to initiate such Treatment); or (b) escaped from a Correctional Institution or from lawful custody.

The information that may be disclosed to avert a serious threat is limited to that listed in section L(1)(b) above. The Office of Legal Counsel or University Privacy Official should be consulted before any Disclosures of PHI are made pursuant to this provision.

N. Workers' Compensation. Under the Oklahoma's Workers' Compensation laws, an employer must provide ~~to~~ an injured employee with medical, surgical, or other attendance or Treatment; nurse and hospital service; medicine; crutches; and any apparatus as may be necessary after an injury that occurred during the course of employment. The attending physician is required to supply the injured employee and the employer, within seven (7) days after the examination, with a full examining report of injuries found at the time of examination and proposed Treatment. At the conclusion of the Treatment, the attending physician must supply a full report of the Treatment of the injured employee to the employer.

The attending physician who renders Treatment to the employee must promptly notify the employee and employer or employer's insurer in writing after the employee has reached maximum medical improvement and is released from active medical care. If the employee is capable of returning to modified light duty work, the attending physician must promptly notify the employee and the employer or the employer's insurer in writing and specify what restrictions, if any, must be followed by the employer in order to return the employee to work.

The Oklahoma Workers' Compensation Act contemplates that an employee who participates in the benefits of this Act is deemed to consent to the treating physician making these reports. Thus, patient Authorization is not required. **However, Uses and Disclosures made under this section must be limited only to that Protected Health Information that is relevant to the injury for which Workers' Compensation benefits are sought.**

IV. REFERENCES

A. 45 C.F.R. §164.512 (f); 45 C.F.R. 164.~~513(2~~514(d)(3)(iii).
B. 85 Okla. Stat. 27.
C. 10 Okla. Stat. 7102.

D. 43A O.S. 10-108.
E. 63 Okla. Stat. 1-116.
F. 63 Okla. Stat. 1-317.
G. 63 Okla. Stat. 1-~~323~~311.
~~H. 663~~63 Okla. Stat. 1-550.2

H. , 3.
I. 63 Okla. Stat. 1-543.
J. 63 Okla. Stat. 1-551.1.

UNIVERSITY OF OKLAHOMA

HIPAA Privacy Policies

Subject: Disclosures to Family and Others Involved in Patient's Care	**Page:** 1 of 3
Policy #: Privacy-26 (Uses & Disclosures)	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Last Revised:** ~~04/26/10; 09/14/12; 09/16/13~~January 29, 2016

I. PURPOSE

To ~~articulate~~describe conditions under which family, friends, and others can be notified of a patient's condition. (These conditions do not limit or replace the authority of a Personal Representative to access PHI. See Privacy-02, Personal Representative.)

II. POLICY*

A. Individuals Involved in Care/Payment. University Personnel may Disclose Protected Health Information to a patient's family member, other relative, close personal friend, or any other person identified by the patient, as long as the Protected Health Information Disclosed is **relevant** to that person's involvement with the patient's care or Payment related to the patient's Health Care~~.~~ and if the University Personnel determines that the Disclosure is in a the patient's best interests. If the patient is present or available, the University Personnel must first give the patient the opportunity to agree or object to the disclosure, unless University Personnel can infer from the circumstances that the patient does not object.

B. Notification/Location. University Personnel may Use or Disclose Protected Health Information necessary to notify, or assist in the notification of (including identifying or locating), a family member, a personal representative of the patient, or another person responsible for the care of the patient of the patient's location, general condition, or death~~.~~ and if the University Personnel determines that the Disclosure to be in a the patient best interests. If the patient is present or available, the University Personnel must first give the patient the opportunity to agree or object to the disclosure, unless University Personnel can infer form the circumstances that the patient does not object.

C. Disaster Relief. University Personnel may Use or Disclose Protected Health Information to a public or private entity authorized by law or by its charter to assist in disaster relief efforts. The Protected Health Information that may be released is limited to the patient's location, general condition, or death and if the University Personnel determines that the Disclosure is in a the patient's best interests. If the patient is present or available, the University Personnel must first give the patient the opportunity to agree or object to the disclosure, unless University Personnel can infer from the circumstances that the patient does not object.

D. Decedents. University personnel may Disclose a decedent's PHI to the decedent's family members, other relative, close personal friend, or individual previously identified by the decedent ~~who were~~if the individual was involved in the care or payment of care of the decedent

prior to death, unless University personnel know that doing so would be inconsistent with any prior expressed preference of the decedent. The Protected Health Information that may be disclosed must be limited to that Protected Health Information that is relevant to the individual's involvement in the decedent's care or payment of care.

III. PROCEDURES

A. Patient is Present – If the patient is present for, or otherwise available prior to, a Use or Disclosure to a family member or other as described in paragraph II (A) – (D) above, and has the capacity to make Health Care decisions, University Personnel may Use or Disclose the Protected Health Information if the University Personnel:

1. Obtains the patient's agreement;

2. Provides the patient with the opportunity to object to the disclosure (and the patient does not express an objection) and documents the lack of objection in the patient's medical record; or

3. Reasonably infers from the circumstances, based on the exercise of professional judgment, that the patient does not object to the Disclosure and notes such in the patient's medical records.

University Personnel may elect to use the Authorization ~~for Verbal~~to Release ~~of~~ Protected Health Information Verbally to Others (available on the HIPAA website) as a mechanism for documenting the patient's agreement to verbal Disclosures.

B. Patient is **Not** Present – If the patient is not present, or the opportunity to agree or object to the Use or Disclosure cannot practicably be provided because of the patient's incapacity or an emergency circumstance, University Personnel may, in the exercise of professional judgment, determine whether the Disclosure in II (1) – (4) above is in the best interests of the patient and, if so, Disclose only the Protected Health Information that is directly relevant to the person's involvement with the patient's Health Care.

University Personnel may use professional judgment and experience with common practice to make reasonable inferences of the patient's best interest in allowing a person to act on behalf of the patient to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of Protected Health Information.

C. Best Interests - The following criteria should be considered when determining whether it is in the patient's best interest to Disclose the Protected Health Information to a family member or other:

1. Whether the potential Disclosure is common practice;

2. The nature of the relationship between the parties;

3. The sensitive nature of the information being Disclosed;

4. The ability of the patient to manage necessary tasks (e.g., pick up prescriptions, medical supplies, x-rays, or other forms of Protected Health Information); and

5. Whether an incapacitated patient is a suspected victim of domestic violence and whether the person seeking information about the patient may have abused the patient. In these instances, University Personnel should not Disclose information to the suspected abuser if there is reason to believe that such a Disclosure could cause the patient harm.

D. Verifying Identity - University Personnel are not required to verify the relationship of relatives or other individuals involved in the patient's care, unless they have reason to doubt the relationship. University Personnel should inquire into the individual's relationship with the patient and document it. The patient's act of involving the other person in his/her care also may suffice as verification of identity.

University Personnel should contact the office of Legal Counsel or the University Privacy Official if they have questions regarding releases under this policy.

IV. REFERENCES

A. HIPAA Privacy Regulations, 45 C.F.R. 164.510(b).

UNIVERSITY OF OKLAHOMA

HIPAA Privacy Policies

Subject: Business Associates	**Page:** 1 of 2
Policy #: Privacy-27 (Uses & Disclosures)	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Last Revised:** ~~04/26/10; 09/14/12; 09/16/13~~January 29, 2016

I. PURPOSE

To establish requirements regarding Uses and Disclosures of Protected Health Information to Business Associates.

II. POLICY*

A Health Care Component may Disclose Protected Health Information to a Business Associate, and may allow a Business Associate to create, receive, maintain, or transmit Protected Health Information on its behalf, if the Health Care Component ensures that the University has executed an agreement with the Business Associate that contains language requiring the Business Associate to appropriately safeguard the Protected Health Information (a "Business Associate Agreement"), in compliance with HIPAA.

A Business Associate is a person or entity who provides certain functions, activities, or services on behalf of the University that involve the University's Protected Health Information. (See the Business Associate Decision Tree available on the HIPAA website.)

If the University or a Health Care Component knows of a pattern of activity or practice of a Business Associate that constitutes a material breach or violation of the Business Associate's obligation under the Business Associate Agreement, the University (through the Health Care Component or University Privacy Official) must take reasonable steps to cure the breach or end the violation. If such steps are unsuccessful, or cure is not possible, the Business Associate Agreement must be terminated. If termination is not possible, the University Privacy Official must report the problem with the Business Associate ~~must be reported~~ to the Secretary of the Department of Health and Human Services ~~by the University Privacy Official~~.

III. PROCEDURE

A. Health Care Components must identify their Business Associates and bring the need for contractual language to the attention of the Office of Legal Counsel, Purchasing Department, or Office of Research Administration, as appropriate, when the Health Care Component routes a contract for signature or otherwise obtains the Business Associate's services. Health Care Components may not share PHI with a Business Associate until a Business Associate Agreement is in place between the University and the Business Associate.

B. The University Privacy Official is responsible for drafting, implementing, and updating the appropriate Business Associate language and/or agreements to comply with the requirements of HIPAA. Templates are available on the HIPAA webpage. All contracts must be reviewed by the Office of Legal Counsel in accordance with University policies.

C. Questions regarding the status of a vendor or independent contractor as a Business Associate should be forwarded to the Office of Legal Counsel or University Privacy Official. Questions regarding whether a vendor has a Business Associate Agreement in place with the University should be directed to the Purchasing Department. Questions regarding whether any other entities have a Business Associate Agreement in place with the University should be directed to the Office of Research Administration.

Business Associate language must be included in applicable new and renewing contracts.

IV. REFERENCES

A. HIPAA Privacy Regulations, ~~65~~ 45 C.F.R. 164.502(e).
B. HIPAA Privacy Regulations, 45 C.F.R. 164.504(e).
C. HIPAA Privacy Regulations, 45 C.F.R. 164.532.

UNIVERSITY OF OKLAHOMA

HIPAA Privacy Policies

Subject: Marketing	**Page:** 1 of 2
Policy #: Privacy-28 (Uses & Disclosures)	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Revised:** January 29, 2016

I. PURPOSE

To establish requirements pertaining to the Use and Disclosure of Protected Health Information for Marketing purposes.

II. POLICY*

A. Health Care Components must obtain an Authorization for any Use or Disclosure of Protected Health Information for Marketing, **unless** the communication is in the form of: (1) a face-to-face communication made by University Personnel to an individual; or (2) a promotional gift of nominal value provided by the Health Care Component. (The University's Authorization form may be used when Authorization is required.)

If the University has received payment in exchange for making one of those communications, the communication may not be considered Health Care Operations unless; (i) the communication describes only a drug or biologic that is currently being prescribed for the recipient of the communication and any payment is reasonable in amount; (ii) the communication is made by the University and individual Authorization is obtained; or (iii) the communication is made by a Business Associate on behalf of the University and the communication is made consistent with the Business Associate agreement.

"Marketing" is defined as a communication about a product or service that encourages the purchase or use of the product or service.

Marketing does not include communications

- **to provide refill reminders for current medications (if the HCC receives direct or indirect payment for sending the reminder, the payment may not exceed the reasonable cost to the HCC for sending it)**
- **for Treatment ~~purposes~~by a Health Care Provider, such as care coordination, and recommendations for alternate therapies or treatments,~~;~~ health care providers; or care settings (no payments may be received)**
- **~~for health-related products or services provided by the HCC, such as health-related goods or services available only to a health plan enrollee that are not part of the plan~~**
- **for case management or~~,~~ care coordination~~,~~ or for contracting individuals about alternate treatment plans~~,~~ and related functions, to the extent they are not Treatment (no payments may be received)**
- **about the University own products or services**

*Capitalized terms are defined in Privacy-01, Definitions

~~If the University has received payment in exchange for making one of those communications, the communication may not be considered Health Care Operations unless; (i) the communication describes only a drug or biologic that is currently being prescribed for the recipient of the communication and any payment is reasonable in amount; (ii) the communication is made by the University and individual Authorization is obtained; or (iii) the communication is made by a Business Associate on behalf of the University and the communication is made consistent with the Business Associate agreement.~~

B. If the Marketing involves direct or indirect payment to the University or a Health Care Component from a third party whose product or services is being described, the Authorization must state that payment is involved. The University Privacy Official must be contacted to develop or review the proposed Authorization to ensure it complies with this Policy.

University Personnel are prohibited from selling patient lists to third parties and from disclosing Protected Health Information to a third party for the independent Marketing activities of the third party, without first obtaining an Authorization from every patient on the list.

C. The University may not directly or indirectly receive remuneration in exchange for Protected Health Information unless Authorized by the individual. However, that general rule does not apply if the purpose or the remuneration is for:

- Public Health activities;
- Research purposes where the price charged reflects the cost of preparation and transmittal of the information;
- Treatment of the individual;
- Health Care Operations related to the sale, merger, or consolidation of a Covered Entity;
- Performance of services by a Business Associate on behalf of the University;
- Providing the individual with a copy of the Protected Health Information maintained about him/her; or
- Other reasons determined necessary and appropriate by the Secretary of the Department of Health and Human Services.

III. PROCEDURE

A. Any Health Care Component wishing to Use or Disclose PHI for Marketing purposes must contact the University Privacy Official, who will assist in providing a HIPAA compliant Authorization, if required.

B. Authorizations for Marketing must be kept in a patient's medical record for at least six (6) years from the date of signature.

IV. REFERENCES

A. HIPAA Privacy Regulations, 45 C.F.R. 164.501.
B. HIPAA Privacy Regulations, 45 C.F.R. 164.508(a)(3).

UNIVERSITY OF OKLAHOMA

HIPAA Privacy Policies

Subject: Fundraising	**Page:** 1 of 2
Policy #: Privacy-29 (Uses & Disclosures)	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Last Revised:** January 29, 2016

I. PURPOSE

To establish requirements pertaining to the Use and Disclosure of Protected Health Information for fundraising purposes.

II. POLICY*

A. Health Care Components may Use (or Disclose to a Business Associate or an institutionally-related foundation) the following Protected Health Information for the purpose of raising funds (including soliciting gifts or sponsorships) without an Authorization: (~~a~~1) demographic information relating to an individual, including name, address, contact information, age, gender, and date of birth; (~~b~~2) dates of Health Care provided to an individual; (~~c~~3) department of service; (~~d~~4) treating physician information; ~~and~~ (~~e~~5) outcome information; and (6) health insurance status.

Any Use or Disclosure of Protected Health Information for fundraising purposes beyond (~~a~~1) – (~~e~~6) above requires the patient's Authorization. Demographic and outcome information does not include the Use or Disclosure of ~~any~~ information about a patient's illness or Treatment.

B. A patient's demographic information ~~(name, address, contact information, age, gender, date of birth, and insurance status),~~ dates of receipt of Health Care services, department of service, treating physician information, ~~and~~ outcome information, and health insurance status may be Used or Disclosed without the patient's Authorization for fundraising purposes only if the following requirements are met:

~~A~~1. The University's Notice of Privacy Practices contains a statement that the University may contact the patient to raise money for the University; and

~~B~~2. The Notice and all fundraising materials describe in a clear and conspicuous manner the procedures for a patient to opt out of receiving any additional fundraising communications. These procedures must generally include an email address or toll-free phone number as options. If a patient opts out, this choice must be treated as a revocation of Authorization.

III. PROCEDURE

A. A Health Care Component doing fundraising must ensure that all fundraising materials

directed to patients~~,~~ indicate that a patient can opt out of receiving fundraising materials from the University, or from a Business Associate or related foundation acting on the University's behalf, via e-mail or toll-free call to the Health Care Component or to the University's Privacy Official or designee. Contact information must be included.

B. Health Care Components must forward a copy of all opt-out requests to the University Privacy Official, who will maintain a master opt-out list.

C. All Health Care Components must contact the University Privacy Official prior to initiating any fundraising campaigns directed at patients of the Health Care Components to ensure the campaign complies with this Policy and that patients who have indicated that they do not want to receive fundraising materials are not solicited.

D. The University, its foundations, Business Associates, and Health Care Components must treat any election by a patient to opt out of receiving future fundraising communications as a revocation of Authorization to use the patient's Protected Health Information for fundraising purposes. Failure to observe the revocation may result in a HIPAA violation.

E. The University and its Health Care Components may not condition Treatment or Payment on an individual's choice to opt-out of any fundraising.

Note: If a Health Care Component uses a public directory or other database not related to the PHI maintained by the Health Care Component or University, ~~these procedures do~~this Policy does not apply. The University Privacy Official should be contacted if the Health Care Component is not sure whether this exception applies.

IV. REFERENCES

A. HIPAA Privacy Regulations, 45 C.F.R. 164.514(f). ~~and~~
B. HIPAA Privacy Regulations, 45 C.F.R. 164.520(b).

UNIVERSITY OF OKLAHOMA

HIPAA Privacy Policies

Subject: Research	**Page:** 1 of 2
Policy #: Privacy-30 (Uses & Disclosures)	**Approved:** March 8, 2012
Effective Date: March 8, 2012	**Last Revised:** January 29, 2016

I. PURPOSE

To establish permitted Uses and Disclosure of PHI in Research.

II. POLICY*

A Health Care Component may Use and Disclose PHI for the purposes of Research only in accordance with University's Office of Human Research Participant Protection (HRPP) policies~~.~~, including the HRPP HIPAA Policies. The University's Institutional Review Board shall serve as the University's Privacy Board. "Research" is defined under HIPAA as a systematic investigation, including research development, testing, and evaluation designed to develop or contribute to generalizable knowledge.

The Use or Disclosure of PHI in Research requires one of the following, in accordance with HRPP policies:

a. Authorization for the Use of Disclosure of PHI;
b. Waiver of the Authorization requirement by the Privacy Board;
c. De-identification of the PHI; or
d. Use of a Limited Data Set, with accompanying Data Use Agreement (available on the HIPAA forms webpage and from the Human Research Participant Protection Office.)

Authorizations must comply with ~~45 C.F.R. §164.508~~Privacy – 23, Authorizations, and HRPP policies.

III. PROCEDURE

A. All Research that will involve the Use or Disclosure of PHI, including for reviews prepatory to Research, must be submitted to the Privacy Board and must be accompanied by the appropriate IRB HIPAA Privacy forms. Revisions to these forms must be approved by the Privacy Board and University Privacy Official.

B. The Privacy Board will determine whether the proposed Use or Disclosure of PHI complies with the applicable provisions of HIPAA~~.~~ and HRPP policies. It may seek input from the Director of Compliance and/or the University Privacy Official.

C. Research involving the Use or Disclosure of De-Identified Health Information or Limited

Data Sets must comply with HRPP policies as well as Privacy-31, Limited Data Sets, and Privacy-32, De-Identified information.

D. Persons conducting Research involving PHI are responsible for logging Disclosures, pursuant to Privacy-06 (Accounting of Disclosures).

IV. REFERENCES

A. HIPAA Privacy Regulations, 45 CFR § 164.512(i).
B. Office of Human Research Participant Protection, SOP 1001, and related forms.

UNIVERSITY OF OKLAHOMA

HIPAA Privacy Policies

Subject: Limited Data Sets	**Page:** 1 of 2
Policy #: Privacy-31 (Uses & Disclosures)	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Last Revised:** January 29, 2016

I. PURPOSE

To establish permitted Uses and Disclosures of limited data sets -- PHI from which specified identifiers have been removed -- and the method for creating them.

II. POLICY*

A Health Care Component may Use and Disclose a limited data set without patient Authorization only for the purposes of Research, public health, or Health Care Operations and only if the Health Care Component enters into a Data Use Agreement with the intended recipient of the limited data set.

A Health Care Component may use Protected Health Information to create a limited data set or Disclose Protected Health Information to a Business Associate to create a limited data set on behalf of the Health Care Component.

If a Health Care Component knows of a pattern of activity or practice of the limited data set recipient that constitutes a material Breach or violation of the Data Use Agreement, it must take reasonable steps to cure the Breach or end the violation, as applicable. If such steps are unsuccessful or the Breach cannot be cured, the Health Care Component must discontinue Disclosure of Protected Health Information to the recipient and report the problem to the University Privacy Official, for report to Secretary of the Department of Health and Human Services.

If a Health Care Component is a limited data set recipient, it must comply with the terms of the Data Use Agreement and this policy.

A limited data set is Protected Health Information that does not directly identify the patient, but contains certain potentially identifying information.

III. PROCEDURE

A. Limited Data Set. In order to create a limited data set, the following direct identifiers of the patient or of relatives, employers, or household members of the patient must be removed:

1. Names
2. Postal address information, other than town, city, state, and zip code/geocode
3. Telephone numbers

*Capitalized terms are defined in Privacy-01, Definitions

4. Fax numbers
5. Electronic mail addresses
6. Social Security Numbers
7. Medical record numbers
8. Health plan beneficiary numbers
9. Account numbers
10. Certificate/license numbers
11. Vehicle identifiers and serial numbers, including license plate numbers
12. Device identifiers and serial numbers
13. Web Universal Resource Locators (URLs)
14. Internet Protocol (IP) address numbers
15. Biometric identifiers, including fingerprints and voiceprints
16. Full-face photographs and comparable images

The patient's birth date should be Disclosed only if the University and the recipient of the information agree that it is needed for their purpose.

B. Data Use Agreements. All Data Use Agreements must be approved by the University Privacy Official or Office of Legal Counsel prior to execution. ~~A sample Data Use Agreement is available on the HIPAA forms webpage and from the University Privacy Official.~~ A Data Use Agreement must:

1. Establish the permitted Uses and Disclosures of the limited data set.

2. Establish who is permitted to Use or receive the limited data set.

3. Provide that the recipient of the information will:

- Not Use or further Disclose the information other than as permitted by the Data Use Agreement or Required by Law
- Use appropriate safeguards to prevent Use or Disclosure of the information other than as permitted by the ~~agreement~~Data Use Agreement
- Report to the University any Uses or Disclosures the recipient is aware of that are not provided for by the Data Use Agreement
- Ensure that the recipient's agents who have access to the information agree to the same restrictions as imposed on the recipient
- Not Use the information to identify the information or contact the individuals
- Not Use or Disclose the information in a manner that would violate HIPAA if done by the Health Care Component or University.

C. Failure to Comply. Health Care Components must report any violations of this Policy or a Data Use Agreement to the University Privacy Official, whether the violation is caused by the Health Care Component or the other party to the Data Use Agreement.

IV. REFERENCES

A. HIPAA Privacy Regulations, 45CFR § 64.514 (e).
~~B. Sample Data Use Agreement – available on the HIPAA forms webpage and from the University Privacy Official~~

UNIVERSITY OF OKLAHOMA

HIPAA Privacy Policies

Subject: De-Identified Information/Re-Identification	**Page:** 1 of 3
Policy #: Privacy-32 (Uses & Disclosures)	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Last Revised:** January 29, 2016

I. PURPOSE

To establish the method and policy for de-identifying and re-identifying Protected Health Information.

II. POLICY*

De-Identified Information/Re-Identification

Health Care Components can Use and Disclose de-identified Health Information, defined below, without regard to the Privacy Policies or Regulations as long as the code or other means of identification designed to permit re-identification is not disclosed.

Health Care Components may Use Protected Health Information to create information that is not Individually Identifiable Health Information or Disclose Protected Health Information to a Business Associate to de-identify Health Information on behalf of the Health Care Component. If de-identified information is re-identified, its Use and Disclosure become subject to regulation under the Privacy Policies and Regulations.

Health Information that does not identify an individual and for which there is no reasonable basis to believe that the Health Information can be used to identify the ~~patient~~individual is "de-identified information" and is not individually identifiable ~~or~~so it is not considered Protected Health Information. It is not subject to the requirements of the Privacy Policies or the Privacy Regulations.

III. PROCEDURE

~~A. Deidentification~~
A. De-Identification

Regardless of method of de-identification of PHI used below, if the Health Care Component has actual knowledge that the remaining information can be used alone or in combination with other information to identify the patient, the information is not considered de-identified.

Health Information can be de-identified by using one of the two methods listed below:

1. Removal of Identifiers. The following identifiers of the patient or of the

*Capitalized terms are defined in Privacy-01, Definitions

relatives, employers, or household members of the patient are removed and the University has no actual knowledge that the information could be used alone or with other information to identify the individual:

a. Names

b. All geographic subdivisions smaller than a state, including street address, city, county, precinct, and zip code and equivalent geocodes, except for the initial 3 digits of a zip code if, according to current publicly available data from the Census Bureau:

~~(~~1.~~)~~ the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people, and

~~(~~2.~~)~~ the initial 3 digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000 (example, for the zip code 73069, all areas using the zip code beginning with 730 have more than 20,000 in the aggregate).

c. All elements of dates (except year) for dates directly related to the patient, including birth date, admission date, discharge date, date of death; and all ages over 89~~;~~ and all elements of dates (including year) indicative of such age. (Exception: Ages and elements may be aggregated into a single category of age 90 or older.)

d. Telephone numbers

e. Fax Numbers

f. E-mail addresses

g. Social Security Numbers

h. Medical record numbers

i. Health plan beneficiary numbers

j. Account numbers

k. Certificate/license numbers

l. Vehicle identifiers, serial numbers, including license plate numbers

m. Device identifiers and serial numbers

n. Web Universal Resource Locators (URLs)

o. Internet Protocol (IP) address numbers

p. Biometric identifiers, including fingerprints and voiceprints

q. Full face photographic images and other comparable images

r. All other unique identifying numbers, characteristics, or codes (except as permitted by III B).

2. Alternative Method of De-Identification. ~~A biostatician or other~~A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable must apply such principles and methods and determine that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify the individual who is the subject of the information. The person making this determination must be an independent third party and must document the methods and results of the analysis that justify the determination.

B. **Re-Identification**

A Health Care Component may assign a code or other means of record identification to allow de-identified information to be re-identified, provided that:

1. Derivation. The code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; and

2. Security. The code and/or mechanism for re-identification is not Used or Disclosed for any other purpose.

IV. REFERENCES

A. HIPAA Privacy Regulations, 45 C.F.R. 164.502(a).~~;~~
~~A.~~B. HIPAA Privacy Regulations, 45 C.F.R. 164.514 (a) – (c).

UNIVERSITY OF OKLAHOMA

HIPAA Privacy Policies

Subject: Breach of Unsecured PHI	**Page:** 1 of 4
Policy: Privacy-34 (Uses & Disclosures)	**Approved:** September 23, 2009
Effective Date: September 23, 2009	**Last Revised:** January 29, 2016

I. PURPOSE

To provide for notification in the case of ~~breaches~~Breaches of unsecured Protected Health Information. For purposes of these requirements, "unsecured Protected Health Information" means Protected Health Information that is not secured through the use of approved technologies or methodologies that render Protected Health Information unusable, unreadable, or indecipherable to unauthorized individuals.

This Policy establishes the requirements regarding the protection of PHI that each Health Care Component must comply with and the notification that must occur in the event of a Breach of unsecured PHI.

II. POLICY*

The University, through its Information Technology and Health Care Components, as applicable, will implement reasonable and appropriate technologies and methodologies designed to secure Protected Health Information from unauthorized Disclosure.

If PHI is rendered unusable, unreadable, or indecipherable to unauthorized individuals, then the PHI is not "unsecured" PHI.

III. PROCEDURE

~~This Policy establishes the requirements regarding the protection of PHI that each Health Care Component must comply with and the notification that must occur in the event of a Breach of unsecured PHI.~~

Each Health Care Component shall designate and document an individual to be responsible for compliance with this Policy, in coordination with the University Privacy Official and HIPAA Security Officer.

A. Methods of Protection – Either of the following methods may be used to secure PHI and make it unusable, unreadable, or indecipherable to unauthorized individuals.

1. **Encryption** – Each Health Care Component will comply with the encryption technologies and methodologies implemented by Information Technology ~~Security~~ to

enhance the protection of PHI and adopted by the University or Health Care Component.

a. Refer to University Information Security policies (available on the Information Technology webpage) for encryption requirements.

2. **Destruction** – Each Health Care Component will comply with the destruction techniques implemented by IT Security and the University Privacy Official that render PHI unusable and/or unreadable in any format.

a. Electronic PHI – Refer to University Security policies (available on the Information Technology webpage~~)~~ http://it.ouhsc.edu/policies) for destruction requirements of electronic PHI.

b. Documents - Refer to Privacy-18, Safeguards, for destruction requirements of paper records containing Protected Health Information.

PHI secured by one of the above methods is not unsecure ~~and is therefore not subject to this Policy~~.

~~For additional information on the guidelines and standards of encryption and destruction methods of electronic PHI, contact Information Technology or visit http://it.ouhsc.edu/policies.~~

.

B. Notification of Breach

1. If a Breach of PHI is suspected or discovered, the University Privacy Official or designee must be notified immediately. The Privacy Official will determine, using the Privacy Official's Breach Notification Reporting Process, whether and when a notice to the individual, the media, and/or HHS is appropriate and, if so, the content of the notice~~.~~, which must be written in plain language. If the Breach involves electronic PHI, the University Privacy Official or Health Care Component will also notify the HIPAA Security Officer.

2. In the event a Breach of unsecured PHI, the University or its designee may be required to notify each individual whose unsecured PHI has been, or is reasonably believed to have been, inappropriately accessed, acquired, Used, or Disclosed. The University Privacy Official shall make such notice according to the requirements of HIPPA, including:

a. Written notices to the individual (or next of kin or personal representative if the individual is deceased) at the last known address of the individual (or next of kin) by first-class mail (or by electronic mail if agreed to by the individual);

b. In the case in which there is insufficient or out-of-date contact information (excluding for next-of-kin or personal representative), substitute notice shall

be provided. In cases of fewer than 10 individuals for whom there is insufficient or out-of-date contact information, substitute notice may be by an alternative form of written notice, telephone, or other means.

c. In the case of 10 or more individuals for whom there is insufficient contact information, conspicuous posting for 90 days consecutive days on the home page of the web site of the University (and of the Health Care Component, if it maintains one) and/or notice in major print or broadcast media, each including a toll-free number that is active for at least 90 days, will occur, as determined by the University Privacy Official.

d. In cases that the Health Care Component or University Privacy Official deem urgent based on the possibility of imminent misuse of the unsecured PHI, the University Privacy Official may require notice by telephone or other method ~~is permitted~~, in addition to the above methods.

e. In cases involving more than 500 residents of a state or jurisdiction, the University Privacy Official shall comply with the requirements of the Privacy Regulations regarding notification to the media.

3. Details of the notice, which must be approved by the University Privacy Official, shall include the following: (A sample letter is available from the University Privacy Official.)

   a. A brief description of what happened, including the date of the Breach and the date of the discovery of the breach, if known;

   b. A description of the types of unsecured PHI that were involved in the Breach (such as full name, SSN, DOB, home address, account number, diagnosis, or disability code);

   c. ~~The~~Any steps individuals should take to protect themselves from potential harm resulting from the Breach;

   d. A brief description of what the Health Care Component involved is doing to investigate the Breach, mitigate ~~losses~~harm to the individual, and protect against any further Breaches;

   e. Contact procedures for individuals to ask questions or ~~learn~~obtain additional information, which shall generally include a toll-free telephone number, an e-mail address, web site, or postal address.

4. If a Breach is caused or discovered by a Business Associate of the University, the University Privacy Official shall work with the Business Associate to address the notice requirements, in accordance with the terms of the Business Associate

Agreement in place between the parties and HIPAA. The timing and content of any required notice shall be in accordance with the Agreement and applicable law.

5. If a Law Enforcement Official informs the University or its Business Associate that a required notice would impede a criminal investigation or threaten national security, the University Privacy Official shall (a) comply with Law Enforcement's written request for a delay for the time period specified in the statement or (b) document Law Enforcement's verbal request, specifying the time for which the delay is required and the identity of the Law Enforcement Official making the request and delay the notice for up to 30 days, unless a written statement with a longer delay period is provided.

C. Tracking

1. Health Care Components must maintain a log of Breaches of unsecure PHI and notify the University Privacy Official of each Breach.

2. The University, through the University Privacy Official, shall maintain a log of all reported Breaches of unsecure PHI and shall submit required reports of such to the Secretary of HHS annually, and as required by the ~~Act~~Privacy Regulations.

IV. REFERENCES

1. HIPAA Privacy Rules 45 CFR ~~Parts~~ 164.400, et seq.
2. NIST SP 800-111 *"Guide to Storage Encryption Technologies for End User Devices"* and SP 800-88 *"Guidelines for Media Sanitization"* as updated or revised.
3. 24 O.S. 163.5 Breach Notification Reporting Process (available from the University Privacy Official).
4. Sample Notice Letter (available from the University Privacy Official).
5. Information Technology Security policies http://it.ouhsc.edu/policies.
6. HITECH Act, Section 13402 of Title XIII of the American Recovery and Reinvestment Act of 2009~~,~~ (effective February 17, 2009); 78 Fed Red 5695, Jan 25, 2013.

UNIVERSITY OF OKLAHOMA

HIPAA Privacy Policies

Subject: Privacy Compliance Audit Program	**Page:** 1 of 2
Policy #: Privacy-35 (Admin.)	**Approved:** December 1, 2012
Effective Date: 12/1/2012	**Last Revised:** ~~January 29~~February 1, 2016

I. PURPOSE

To formalize the University's HIPAA Privacy Compliance Audit Program[1].

II. POLICY*

The University Privacy Official, in coordination with the Office of Compliance, will maintain a HIPAA Privacy Audit Program to promote HIPAA awareness and compliance. (The Program may include HIPAA ~~s~~Security audit items as well, with the cooperation of the HIPAA Security Officer and the Office of Compliance.)

Documentation of all audits shall be maintained by the University Privacy Official and/or Office of Compliance for at least six (6) years.

III. PROCEDURE

A. The Office of Compliance shall employ a HIPAA Compliance Auditor, who shall conduct and/or coordinate HIPAA compliance audits under the direction of the University Privacy Official. Audit instruments will be updated as needed by the University Privacy Official and Office of Compliance to address current and ongoing HIPAA issues.

B. The HIPAA Privacy Audit Program shall include, at a minimum, the following:

1. In-person audits of each Health Care Component clinic, occurring approximately once every 12 months, or more often if indicated by audit results or HIPAA incidents, and of each Health Care Component departmental office, occurring approximately once every 24 months, or more often if indicated by audit results or HIPAA incidents.

2. Quarterly self-audits of each Health Care Component using a self-audit instrument developed and maintained by the University Privacy Official and Office of Compliance, or more often if indicated by audit results or HIPAA incidents.

3. In-person audits of local off-site facilities where PHI is physically stored by a

[1] For policies and procedures on the audit program for Electronic Medical Records systems, refer to the HIPAA Security Audits policy.

Health Care Component, occurring approximately every ~~12 months~~2 years, or more often if indicated by audit results or HIPAA incidents. The off-site facilities may be audited via written compliance certification between in-person audits.

4. Coordination with the University's Internal Audit Department on HIPAA audit issues, items, and findings.

5. Regular audits of the University's Business Associates, either in person or via written compliance certification.

C. The HIPAA Compliance Auditor shall submit a copy of the audit reports from each in-person audit to the University Privacy Official, generally within two weeks of ~~conducting~~ the audit. If HIPAA Security issues were identified, the HIPAA Security Officer will also receive a copy.

D. The University Privacy Official and, if applicable, the Security Officer will provide the Director of Compliance with a written response, including recommended corrective action, to each in-person audit report, generally within two weeks of receipt of the report. The Director of Compliance shall timely notify each Health Care Component in writing of the audit results, including any corrective action required. The Director shall confirm corrective action is taken, as required. The University Internal Auditor and appropriate Health Care Component administrators shall receive a copy of the Director's letter.

E. The HIPAA Compliance Auditor shall review the quarterly self-audits and timely notify the Health Care Component or University Privacy Official if the audit indicates the need for corrective action or additional training. The University Privacy Official shall coordinate such training or action with the Compliance Auditor or appropriate individual.

F. The University Privacy Official shall notify the affected Health Care Component if any Business Associate fails to comply with the University's audit request or if the audit results indicate HIPAA deficiencies, necessitating termination of the Business Associate arrangement and/or reporting to the Secretary of Health and Human Services.

G. The University Privacy Official shall regularly review this Policy and make revisions as necessary to ensure it continues to appropriately evaluate HIPAA Privacy compliance.

IV. REFERENCES

A. HIPAA Privacy Regulations, 45 CFR §164.306.
B. HIPAA Security Audits policy.