

**UNIVERSITY OF OKLAHOMA**

**HIPAA Privacy Policies**

<b>Subject:</b> Introduction	<b>Coverage:</b> Health Care Components
<b>Policy #:</b> Privacy-00	<b>Page:</b> 1 of 1
<b>HIPAA Section:</b>	<b>Approved:</b> October 8, 2002
<b>Effective Date:</b> April 1, 2003	<b>Revised:</b>

**I. POLICY**

It shall be the policy of the University<sup>1</sup> 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 and applicable state laws.

The Policies contained in this manual 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 to effectuate these Policies.

These Policies will apply to all protected health information collected by Health Care Components after April 14, 2003. The Policies apply to all University Personnel.

The Policies supercede and replace any existing policies and procedures of any Health Care Component relating to the use and disclosure of protected health information. Health Care Components only can maintain separate policies and procedures relating to the use and disclosure of health information to the extent that they do not conflict with these Policies. Health Care Components can add to or supplement the Policies or the forms attached hereto, but may not delete anything without first consulting with the Privacy Official.

**These Policies apply to all health information, regardless of the form in which it is created or maintained (i.e., whether oral, written or electronic).**

**These Policies apply to the health information of both living and deceased patients.**

<sup>1</sup> The University is a Hybrid Entity with designated Health Care Components. See, Privacy-01, number 16.

# UNIVERSITY OF OKLAHOMA

## HIPAA Privacy Policies

<b>Subject:</b> Definitions	<b>Coverage:</b> Health Care Components
<b>Policy #:</b> Privacy-01 (Definitions)	<b>Page:</b> 1 of 7
<b>HIPAA Section:</b> 164.510(a)	<b>Approved:</b> October 8, 2002
<b>Effective Date:</b> April 1, 2003	<b>Revised:</b> March 1, 2003

### I. DEFINITIONS

Unless otherwise provided, the definitions set forth below apply to all of the Privacy Policies. Certain terms will be capitalized when used in the policies to indicate that they have been uniquely defined by the University.

1. Business Associate. A person or entity not employed by the University that provides certain functions, activities, or services for or on behalf of the University, which involves the use and/or disclosure of a patient's protected health information. Such activities may include, but are not limited to, billing, repricing, claims processing and administration, data analysis, legal, accounting, actuarial, consulting, utilization review, quality assurance, and similar services or functions. A business associate may be a covered entity. The definition of a business associate excludes a person who is part of the covered entity's workforce. 45 C.F.R. § 160.103.

2. Compliance Date. The date by which a covered entity must comply with the Privacy Regulations, which is April 14, 2003.

3. 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.

4. Covered Entity. The entities to which the Privacy Regulations apply, which include: (a) a health plan; (b) a health care clearinghouse; and (c) a health

care provider who transmits any health information in electronic form in connection with one of the following eleven (11) 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.

5. 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.

6. Designated Record Set. A group of records maintained by or for a University Health Care Component that includes the medical and billing records about individuals or that are 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 purposes; (d) psychotherapy notes; (g) information compiled in reasonable anticipation of litigation or administrative action; (h) employment records; (i) student records; and (j) source data interpreted or summarized in the individual's medical record (example: pathology slide and diagnostic films).

**This definition refers only to the official record for the patient and not to duplicate information maintained in other systems. 65 Fed Reg. 82559.**

7. 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. § 164.501.

**Exchange of protected health information with a department of the University that is not designated as a Health Care Component is considered a disclosure.**

8. 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.

9. 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.

10. Health Care Component(s). A component or combination of components designated by the University, which is a hybrid entity. The “health care components” of the University of Oklahoma include the: (i) College of Medicine – Oklahoma City, including OU Physicians; (ii) the College of Medicine – Tulsa, including OU Physicians-Tulsa; (iii) College of Pharmacy; (iv) College of Dentistry; (v) College of Nursing; (vi) College of Allied Health; (vii) College of Public Health; (viii) Goddard Health Center; (ix) George Nigh Rehabilitation Institute; (x) the Athletic Department; (xi) Internal Auditing; (xii) the Office of Legal Counsel; (xiii) the General Clinical Research Center; (xiv) HSC Financial Services; (xv) NC Financial Support Services; (xvi) Office of Compliance; and (xvii) Human Research Participant Protection Program/Institutional Review Board.

**As this term 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) and University Personnel providing health care services on behalf of the University.**

11. 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, 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.

12. 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.

13. 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.

14. Health Oversight Agency. An agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or 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.

15. HIPAA. The Health Insurance Portability and Accountability Act of 1996.

16. 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.

17. 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.

18. Individually Identifiable Health Information. Information that is a subset of health information, including demographic information collected from an individual, and; (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 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. § 160.503

19. Inmate. A person incarcerated in or otherwise confined to a correctional institution. 45 C.F.R. § 164.501.

20. 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. § 164.501.

21. Legal Counsel. The University's Office of Legal Counsel and the attorneys that work therein.

22. 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.

23. 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.

24. 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.

25. Payment. Any activities by the University, or a Health Care Component, to obtain for providing health care. Such activities relate to the individual to whom health care is provided and included, 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 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.

26. Protected Health Information or PHI. Individually identifiable health information that is transmitted by, or maintained in, electronic media or any other form or medium.

**Protected health information excludes individually identifiable health information in: (a) education records covered by the Family Educational Rights and Privacy Act (FERPA); and (b) employment records held by the University in its role as employer.**

27. Privacy Policies or Policies. This set of policies and procedures drafted and adopted by the University for the use of its Health Care Components relating to the protection and confidentiality of protected health information.

28. 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, 42 CFR Parts 160 and 164, and are aimed at protecting a patient's right to privacy in matters involving his or her health care.

29. 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* excludes medication prescription and monitoring, counseling sessions 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.**

30. Public Health Authority. An agency or authority of the United States,

a State, a territory, a political subdivision of a State or territory, or 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.

31. Required by Law. A mandate contained in law that compels an entity 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 summons issued by a court, grand jury, a governmental or tribal inspector general, or an 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 statutes or regulations that require such information if payment is sought under a government program providing public benefits. 45 C.F.R. § 164.501.

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

33. 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 care provider to another. 45 C.F.R. § 164.501.**

34. University. The University of Oklahoma.

35. University Personnel. Faculty, staff, volunteers, students and other trainees, volunteers, and other persons whose conduct, in the performance of work for the University, is under the direct control of the University, whether or not they are paid by the University. 45 C.F.R. § 160.103.

36. 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.

# UNIVERSITY OF OKLAHOMA

## HIPAA Privacy Policies

<b>Subject:</b> Personal Representatives	<b>Coverage:</b> Health Care Components
<b>Policy #:</b> Privacy-02 (Uses & Disclosures)	<b>Page:</b> 1 of 3
<b>HIPAA Section:</b> 164.510(a)	<b>Approved:</b> October 8, 2002
<b>Effective Date:</b> April 1, 2003	<b>Revised:</b>

### I. PURPOSE

To establish who can act on behalf of the patient for purposes of authorizing uses and disclosures and effectuating the patient rights afforded by these Policies.

### II. POLICY

A Health Care Component must, except in the limited circumstances set forth in this Policy, treat a personal representative as the patient for purposes of authorizing uses and disclosures and effectuating the patient rights afforded by these Policies. *However, the personal representative must only be treated as the individual patient 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 individual 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 personal representative, University Personnel are not required to do so. See, Privacy-05, Patient Access to Protected Health Information.

#### Adults

The following can act as a personal representative of an adult:

1. Durable Power of Attorney for Health Care. A durable power of attorney is a document by which the patient may designate another as his/her agent to perform certain acts on behalf of the patient. Pursuant to 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. This does not give the agent the power to execute on behalf of the patient an advance directive for health care, living will, or other document purporting to authorize life-sustaining treatment decisions, or 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 principal that the authority conferred will be exercisable notwithstanding the principal’s subsequent disability or incapacity. The document should state whether University Personnel may rely on the power of attorney while the patient is still competent or whether it is only effective 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 be witnessed by two witnesses who are at least 18 years old. The signature of the patient and witnesses should 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 withdrawal of life-sustaining treatment, in certain circumstances pursuant to an advanced directive for health care decision. In particular, a health care proxy’s authority only becomes effective (i) when the patient is incompetent and (ii) when the patient 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 communication of the desire to revoke to the attending physician or other University Personnel. If the patient revokes the advanced directive, a health care proxy may not longer qualify 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. Experimental Treatment Statute. This statute, 63 Okla. Stat. 3102A, provides that a legal guardian, attorney-in-fact, and certain enumerated family members can consent to a patient’s participation in a research study being conducted by a University faculty member that has received IRB approval.

## **Minors**

For minor patients who are under the age 18 and who do 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 minor’s personal representative.

A minor may act on his/her own behalf 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, 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, suffering from a communicable disease, drug or substance abuse, nor 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.

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.

### **Deceased Individuals**

A court-appointed executor, administrator, or personal representative of the deceased's estate can act on behalf of a deceased individual. The court document is known as the Letters Testamentary or Letters of Administration and should be signed by a judge.

### **III. PROCEDURES**

1. 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 Legal Counsel.

2. A copy of the written document appointing a person as the personal representative of a patient must be placed in the patient's medical record as verification of the individual's authority.

### **IV. REFERENCES**

- 1. 58 Okla. Stat. 1072.1, 63 Okla. Stat. 3101.1, 63 Okla. Stat. 3102A, 63 Okla. Stat. 2602

# UNIVERSITY OF OKLAHOMA

## HIPAA Privacy Policies

<b>Subject:</b> Verification	<b>Coverage:</b> Health Care Components
<b>Policy #:</b> Privacy-03 (Uses & Disclosures)	<b>Page:</b> 1 of 2
<b>HIPAA Section:</b> 164.514(h)	<b>Approved:</b> October 8, 2002
<b>Effective Date:</b> April 1, 2003	<b>Revised:</b>

### I. PURPOSE

To establish an identity verification process.

### II. POLICY

Prior to making a disclosure or processing a patient right request permitted by these Policies, 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 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.

University Personnel may rely on:

- a. 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.
- b. Appropriately executed documentation of an IRB or Privacy Board waiver or alteration of the authorization requirement.
- c. A request by a 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.
- d. Personal judgment if a disclosure is being made to avert a serious threat to health or safety or in cases when a patient is only required to be given an opportunity to agree or object.

### **III. PROCEDURES**

Any questions regarding verification or reliance on identity or authority should be directed to Legal Counsel. Legal Counsel should be contacted prior to responding to any request by law enforcement officials if possible.

**Verification of identity can be accomplished by: (1) presentation of picture I.D.; (2) signature comparison; or (3) some other appropriate method.**

# UNIVERSITY OF OKLAHOMA

## HIPAA Privacy Policies

<b>Subject:</b> Notice of Privacy Practices	<b>Coverage:</b> Health Care Components
<b>Policy #:</b> Privacy-04 (Patient Rights)	<b>Page:</b> 1 of 3
<b>HIPAA Section:</b> 164.520	<b>Approved:</b> October 8, 2002
<b>Effective Date:</b> April 1, 2003	<b>Revised:</b>

### I. PURPOSE

To require the development of a Notice of Privacy Practices and to provide for general distribution procedures.

### II. POLICY

The University will develop and distribute a Notice of Privacy Practices for its Health Care Components that includes the information required by § 164.520 of the Privacy Regulations. A copy of the Notice of Privacy Practices will be attached hereto as Form – 04. A Health Care Component may develop its own Notice of Privacy Practices. If a Health Care Component elects to develop its own Notice of Privacy Practices, it must obtain the approval of the Privacy Official before publishing it or revising it. A patient's receipt of the Notice of Privacy Practices must be acknowledged as required by the Privacy Regulations.

The Notice of Privacy Practices must be translated into other languages as required by regulations issued by the Federal Office of 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

#### Acknowledgement

If the patient does not acknowledge receipt of the Notice of Privacy Practices, a note should be made on the registration form or in the patient's medical record indicating why the acknowledgement was not obtained. Health Care Components should not condition treatment on the patient's acknowledgement of the receipt of the Notice of Privacy Practices.

University Personnel must make a good faith effort to obtain a written acknowledgement from the patient of his/her receipt of the Notice of Privacy Practices. Each Health Care

Component can determine how to obtain a patient's acknowledgement depending on its particular operational requirements.

**However, the preferred method for obtaining acknowledgement is to require the patient to initial or sign the following statement which should be included on registration and/or encounter forms: "I acknowledge that I have received a copy of the University's Notice of Privacy Practices and I consent to the use of my protected health information for treatment, payment and the healthcare operations of the University as summarized in the Notice of Privacy Practices."**

If the patient does not acknowledge receipt of the Notice of Privacy Practices, a note should be made on the registration form or in the patient's medical record indicating why the acknowledgement was not obtained. Health Care Components should not condition treatment on the patient's acknowledgement of the receipt of the Notice of Privacy Practices.

## **Distribution**

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 current patient of the University.

2. In addition, the 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 after the compliance date, including service delivered electronically. If the first service delivery to an individual is delivered electronically, a provider must provide an electronic copy of the Notice of Privacy Practices automatically and contemporaneously in response to the individual's first request for service.

**During emergency treatment situations, the Notice of Privacy Practices may be provided and the acknowledgement obtained time reasonably practicable after the emergency treatment situation 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 the notice.

3. The Notice may be distributed by e-mail, if the patient agrees to the electronic notice and the agreement has not been withdrawn. All timing requirements still 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 must be obtained.

4. Health Care Components must ensure that health care providers with **indirect** treatment relationships with patients provide the Notice of Privacy Practices to individuals upon request.

5. The Notice of Privacy Practices for the Health Care Components must be posted and made available electronically on the web site of the Health Sciences Center, both Oklahoma City and Tulsa campuses, and of Goddard Health Center. 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.

### **Amendment**

If the Notice of Privacy Practices is amended, it must be made available upon request on or after the effective date.

### **Retention**

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

## **IV. REFERENCES**

1. AMC HIPAA Privacy Guidelines, PRIV. 43 (pg. 167-172).
2. HIPAA Privacy Regulations, 65 Fed. Reg. 82547–52, 82720-26 (December 28, 2000) and 67 Fed. Reg. 53238-53243 (August 14, 2002).

# UNIVERSITY OF OKLAHOMA

## HIPAA Privacy Policies

<b>Subject:</b> Patient Access to Protected Health Information	<b>Coverage:</b> Health Care Components
<b>Policy #:</b> Privacy-05 (Patient Rights)	<b>Page:</b> 1 of 4
<b>HIPAA Section:</b> 164.524(a)	<b>Approved:</b> October 8, 2002
<b>Effective Date:</b> April 1, 2003	<b>Revised:</b>

### I. PURPOSE

To permit patients access to their protected health information.

### II. POLICY

#### Rights to Access

The University will permit patients to inspect and obtain a copy of protected health information about the patient included in a designated record set maintained by a Health Care Component(s), 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.

**Unless an exception applies, a patient should be granted access to the entire medical record, 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 only includes the costs of copying and postage and is consistent with any limit set by State law.

**State law permits a charge of \$1.00 for the first page and \$.50 for each subsequent page for paper records and \$5.00 per film for radiology films.**

The University must provide the patient with access to 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 such other form or format as agreed to by the University and the patient.

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 a copy of the information at the patient's request. 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 knows where the requested information is maintained, the University must inform the patient where to direct the request for access.

### **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, definition of psychotherapy notes in Privacy-01, Definitions (number 23) and Privacy-24, Mental Health.

### **Denial of Right to Access**

A patient may be denied access 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 Legal Counsel should be obtained prior to denying a patient's request for access.
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 such copy 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 responsible for the transporting of 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 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 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 if the protected

health information 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 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.

The University must, to the extent possible, give the patient access to any other protected health information requested, after excluding the protected health information as to which access is being denied.

8. Psychotherapy Notes. See, preceding section of this policy.

### **Review of Denied Access**

If access is denied for the reasons set forth in Number 5, 6 and 7 above, the patient must be given the opportunity to have the denial reviewed by the medical director of 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.

## **III. PROCEDURES**

### **Rights to Access**

1. Patients must make their requests for access in writing using the form attached hereto as Form-05.A. Patients making their request for access by telephone or e-mail should be forwarded a copy of the form. **Verification of the requester's identity must be obtained prior to granting access.** The request form must be maintained in the patient's medical record for a minimum of six (6) years.

2. Any Health Care Component that receives a request for access should provide the patient with the form attached hereto as Form-05.A. 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 immediately forward a copy of the request to the 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 process the request and send a copy of the request form and a copy of the denial letter, if applicable, 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) days after receiving the request.

4. Each Health Care Component must designate and document the titles of persons or offices responsible for receiving and processing requests for access by individual. A copy of the designations must be provided to Legal Counsel. The Health Care Components must update the lists as changes are made and provide an updated list to the Privacy Official. The Privacy Official must 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 Legal Counsel.

### **Denial of Right to Access**

If a patient's request for access is denied, the individual must be provided with a written denial using the form attached hereto as Form-05.B. The denial form must be maintained in the patient's medical record for a minimum of six (6) years. The copies forwarded to the Privacy Official also should be maintained for six (6) years.

### **Review of Denied Access**

Health Care Components are required to promptly forward requests for review to the Reviewer and 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 must be provided to the patient in accordance with the determination of the Reviewer who reviewed the request. The patient making the request should be notified promptly, in writing, of the Reviewer's decision.

## **IV. REFERENCES**

1. AMC HIPAA Privacy Guidelines, PRIV. 45 (pg. 175).
2. HIPAA Privacy Regulations, 65 Fed. Reg. 82554, 82731 (December 28, 2000).

**The health care provider that treated the patient should be notified if a patient requests access to his/her protected health information for litigation or some other unusual purpose.**

# UNIVERSITY OF OKLAHOMA

## HIPAA Privacy Policies

<b>Subject:</b> Accounting of Disclosures	<b>Coverage:</b> Health Care Components
<b>Policy #:</b> Privacy-06 (Patient Rights)	<b>Page:</b> 1 of 4
<b>HIPAA Section:</b> 164.528(a)	<b>Approved:</b> October 8, 2002
<b>Effective Date:</b> April 1, 2003	<b>Revised:</b>

### I. PURPOSE

To permit patients to request an accounting of the disclosures of their protected health information.

### II. POLICY

The University will permit patients to request an accounting of disclosures of 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.

#### Accounting Requirements – General

The accounting must include all disclosures, **except** for disclosures:

1. to carry out treatment, payment and 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;
4. pursuant to the patient's authorization;
5. for a facility directory or to persons involved in the patient's care;
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; or
9. that occurred prior to the compliance date.

**Examples of disclosures subject to the accounting requirement include 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, etc.**

### **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 for 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 IRB. To use this method of accounting the disclosure must involve at least 50 records.**

### **Suspension of Accounting**

A patient's right to receive an accounting of disclosures may 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 patient's right to receive an accounting from a health oversight agency or law enforcement official, Legal Counsel should be contacted to determine if the appropriate conditions have been satisfied.

### III. PROCEDURE

1. A patient must request an accounting for disclosure in writing using the form attached hereto as Form-06.A. **Verification of the requester's identity must be obtained prior to granting the request for an accounting.** Patients making their request for an amendment by telephone or e-mail should be forwarded a copy of the form. The request form must be maintained in the patient's medical record for a minimum of six (6) years.
2. Any Health Care Component that receives a request for an accounting of disclosures should provide the patient with the form attached hereto as Form-06.A. 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 immediately forward a copy of the request to the 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 process the request and send a copy of the request form and a copy of the accounting of disclosure form to the Privacy Official.
3. Health Care Components should designate an individual or individuals who will be responsible for processing requests for accounts of disclosures.
4. For each disclosure that must be recorded, the accounting must include the following information:
  - a. the date of the disclosure;
  - b. the name of the entity or person who received the protected health information and, if known, the address of such entity or person;
  - c. a brief description of the protected health information disclosed; and
  - d. a brief statement of the purpose of the disclosure that reasonably informs the patient of the basis for the disclosure.
5. The form attached hereto as Form-06.B 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.
6. The Accounting Request Form and any copies of the request form and the accounting

form forwarded to the Privacy Official also should be maintained for six (6) years.

7. 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, provide:

- a. the information set forth in section 2 above for the first disclosure during the accounting period;
- b. the frequency, periodicity, or number of the disclosures made during the accounting period; and
- c. the date of the last such disclosure during the accounting period.

8. The University will act on the patient's request for an accounting, no later than sixty (60) days after receipt of such a request.

9. The first accounting to a patient in any twelve (12) 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 (12) 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.

#### **IV. REFERENCES**

1. AMC HIPAA Privacy Guidelines, PRIV. 47 (pg. 185).
2. HIPAA Privacy Regulations, 65 Fed. Reg. 82559, 82739 (December 28, 2000), 67 Fed. Reg. 53237, 53243, 53247 (August 14, 2002).

# UNIVERSITY OF OKLAHOMA

## HIPAA Privacy Policies

<b>Subject:</b> Communication by Alternative Means	<b>Coverage:</b> Health Care Components
<b>Policy #:</b> Privacy-07 (Patient Rights)	<b>Page:</b> 1 of 2
<b>HIPAA Section:</b> 164.522(b)(1)	<b>Approved:</b> October 8, 2002
<b>Effective Date:</b> April 1, 2003	<b>Revised:</b>

### 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 patient's 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 of an alternative means of communication on: (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

1. A patient must request communication by alternative means or at alternative locations in writing by using the sample form attached hereto as Form-07.
2. Any Health Care Component that receives a request for communications by alternative means or at alternative locations should provide the patient with the form attached hereto as Form-07. 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 immediately forward a copy of the request to the 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 alternative means of communication from any other Health Care Components, the Health Care Component that received the initial request should process the request and send a copy of the request form and the denial form, if applicable, to the Privacy Official..

3. Health Care Components should 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 the expense and administrative burden involved with complying with the request. Questions regarding the reasonableness of a particular request should be forwarded to the Privacy Official.

4. Health Care Components should, if possible, notify the patient making the request in writing at the time of his/her visit if the request is denied by providing the patient with a copy of the form attached hereto as Form-07 with the reason for the denial noted. If the patient cannot be notified of the denial at the time of his/her visit, the form for requesting an alternative means of communication, with the denial noted, should be sent to the patient. **In order to protect the patient, the denial should be sent to the alternative address, if specified.**

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

6. Health Care Components must ensure that agreed upon alternative means of communication are communicated to the billing department and other departments and providers and business associates who may be sending the patient communications on behalf of the Health Care Provider who agreed to the request.

7. If a request for communication by alternative means is granted, a Health Care Component must place or affix a clear indication of the communication by alternative means on the patient's medical record, whether it be paper or electronic.

#### **IV. REFERENCES**

1. AMC HIPAA Privacy Guidelines, PRIV. 44 (pg. 173).

2. HIPAA Privacy Regulations, 65 Fed. Reg. 82553, 82730 (December 28, 2000).

# UNIVERSITY OF OKLAHOMA

## HIPAA Privacy Policies

<b>Subject:</b> Right to Amend Records	<b>Coverage:</b> Health Care Components
<b>Policy #:</b> Privacy-08 (Patient Rights)	<b>Page:</b> 1 of 3
<b>HIPAA Section:</b> 164.526(a)	<b>Approved:</b> October 8, 2002
<b>Effective Date:</b> April 1, 2003	<b>Revised:</b>

### 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, or a particular record, contained in a designated record set.

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:

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;
2. Is not part of the designated record set;
3. Is not available for inspection by the individual pursuant to Privacy-05, Individual Access Policy;
4. Is accurate and complete.

Patients requesting an amendment to their protected health information must provide a reason to support a requested amendment.

### III. PROCEDURE

1. Patients must request amendments to their protected health information in writing by using the form attached hereto as Form-08.A. Patients making their request for an amendment by telephone or e-mail should be forwarded a copy of the form. Verification of the requester's

identity must be obtained prior to considering the amendment request. The request form must be maintained in the patient's medical record for a minimum of six (6) years.

2. Any Health Care Component that receives a request for an amendment should provide the patient with the form attached hereto as Form-08.A. 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 immediately forward a copy of the request to the 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 Components, the Health Care Component that received the initial request should process the request and send a copy of the request form to the Privacy Official.

3. 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, prior to making an amendment decision and should sign the amendment form.

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

a. 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 the amendment to such record; (ii) Inform the patient, in writing, that the amendment is accepted by sending the patient a copy of the form attached hereto as Form-08.A 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 by using the form attached hereto as Form-08.B; and (iv) Make reasonable efforts to inform and 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, including business associates, that the Health Care Component knows have the protected health information that is the subject of the amendment and that may have relied, or could foreseeably rely, on such information to the detriment of the patient.

b. 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 form attached hereto as Form-08.A; (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.

5. If a statement of disagreement has been submitted by the patient, a Health Care Component must include the material set forth in subsection (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.

6. 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.**

7. 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 designated record sets.

8. 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**

1. AMC HIPAA Privacy Guidelines, PRIV. 46 (pg. 181).
2. HIPAA Privacy Regulations, 65 Fed. Reg. 82558, 82736 (December 28, 2000).

# UNIVERSITY OF OKLAHOMA

## HIPAA Privacy Policies

<b>Subject:</b> Right to Request Restriction on Disclosures	<b>Coverage:</b> Health Care Components
<b>Policy #:</b> Privacy-09 (Patient Rights)	<b>Page:</b> 1 of 3
<b>HIPAA Section:</b> 164.522(a)(1)	<b>Approved:</b> October 8, 2002
<b>Effective Date:</b> April 1, 2003	<b>Revised:</b>

### 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 § 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.**

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 that received the information not further use or disclose the information.

Any agreed to restriction will not be effective to prevent uses and disclosures to the patient or required by law.

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

**University Personnel may not use or disclose protected health information subject to a restriction, except to provide emergency treatment or unless required by law.**

### III. PROCEDURE

1. Patients must request restrictions on the use and disclosure of their protected health information in writing by using the sample form attached hereto as Form-09. Patients making their restriction requests by telephone or e-mail should be forwarded a copy of the form.

Verification of the requester's identity must be obtained prior to considering the request. The request form must be maintained in the patient's medical record for a minimum of six (6) years.

2. Any Health Care Component that receives a restriction request should provide the patient with the form attached hereto as Form-09. 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 immediately forward a copy of the request to the 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 process the request and send a copy of the request form to the Privacy Official.

**Requests for restrictions should only be granted in rare instances in which the facts and circumstances indicate such a restriction is necessary to protect the patient.**

3. The Privacy Official should be contacted prior to considering any restriction request.

4. Health Care Components should designate an individual or individuals who will be responsible for determining if a particular restriction will be permitted.

5. Health Care Components must notify the patient making the request in writing at the time of his/her visit if the request is denied by providing the patient with a copy of the form attached hereto as Form-09 with the reason for the denial noted. If the patient cannot be notified of the denial at the time of his/her visit, the form for requesting a restriction, with the denial noted, should be sent to the patient.

6. Requests for restrictions, and documentation of any denials of such requests, should be maintained in a patient's medical record for a minimum of six (6) years.

7. Health Care Components must ensure that agreed upon restrictions on the use and disclosure of protected health information are communicated to the billing department and other departments, providers and business associates who may be sending the patient communications on behalf of the University and/or Health Care Provider who agreed to the request.

8. A restriction on the use and disclosure of protected health information 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 to the Privacy Official; or (c) the University and/or the Health Care Component informs the patient that it is terminating its agreement to a restriction in which case the termination only will apply to protected health information created or received after the patient has been notified of the termination.

9. If a restriction request is granted, a Health Care Component must place or affix a clear indication of the restriction on the patient's medical record, whether it be paper or electronic.

#### **IV. REFERENCES**

1. AMC HIPAA Privacy Guidelines, PRIV. 11 (pg. 96).
2. HIPAA Privacy Regulations, 65 Fed. Reg. 82552, 82726 (December 28, 2000).

# UNIVERSITY OF OKLAHOMA

## HIPAA Privacy Policies

<b>Subject:</b> Privacy Official – Contact Information	<b>Coverage:</b> Health Care Components
<b>Policy #:</b> Privacy-10 (Admin.)	<b>Page:</b> 1 of 1
<b>HIPAA Section:</b> 164.530(a)(1)	<b>Approved:</b> October 8, 2002
<b>Effective Date:</b> April 1, 2003	<b>Revised:</b>

### 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 will 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 complaints regarding compliance with the Policies and the Notice.

### III. PROCEDURE

1. 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 Privacy Official.
2. The contact information for the Privacy Official is set forth on Form-10 and will be revised in the event a new Privacy Official is designated or the contact information changes.

### IV. REFERENCES

1. AMC HIPAA Privacy Guidelines, PRIV. 48 and 49 (pg. 190-193).
2. HIPAA Privacy Regulations, 65 Fed. Reg. 82561, 82744-45 (December 28, 2000).

# UNIVERSITY OF OKLAHOMA

## HIPAA Privacy Policies

<b>Subject:</b> Privacy Complaint Reporting and Tracking	<b>Coverage:</b> Health Care Components
<b>Policy #:</b> Privacy-11 (Admin.)	<b>Page:</b> 1 of 2
<b>HIPAA Section:</b> 164.530	<b>Approved:</b> 7/30/2008
<b>Effective Date:</b> 8/1/2008	<b>Revised:</b> 7/30/2008

### I. PURPOSE

To establish the procedures for individuals to submit privacy incidents regarding the University's Privacy Policies and the alleged failure to comply with such Policies by the University's Health Care Components and/or University Personnel.

### II. POLICY

All incidents regarding the University's Privacy Policies and compliance with such Policies, regardless of the form in which they were received, will be documented, reviewed, and acted upon, if necessary, by the University's Privacy Official.

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

### III. PROCEDURE

1. Each Health Care Component must develop and implement a process for receiving privacy incidents and reporting them to the University's 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. The incident report form is attached as Form-11. The contact information for the University's Privacy Official is located on Form-10. If a particular University Health Care Component would like to keep track of privacy complaints received for quality assurance purposes, the Health Care Component can develop an alternative process, as long such process involves the notification of the University's Privacy Official of each complaint received so that the Privacy Official can record and track the response to each complaint and can participate in the resolution of such complaints.

2. The Privacy Official will document each complaint received and maintain such documentation for the minimum retention period stated above.

3. The Privacy Official will investigate each complaint, in conjunction with the applicable

Health Care Component and, if necessary, in conjunction with other affiliated entities, and will document the resolution of the investigation and any corrective actions taken.

#### **IV. REFERENCES**

1. AMC HIPAA Privacy Guidelines, PRIV. 52 (pg. 198).
2. HIPAA Privacy Regulations, 45 CFR §164.530.

# UNIVERSITY OF OKLAHOMA

## HIPAA Privacy Policies

<b>Subject:</b> Documentation	<b>Coverage:</b> Health Care Components
<b>Policy #:</b> Privacy-12 (Admin.)	<b>Page:</b> 1 of 2
<b>HIPAA Section:</b> 164.530(j)	<b>Approved:</b> October 8, 2002
<b>Effective Date:</b> April 1, 2003	<b>Revised:</b>

### I. PURPOSE

To establish documentation requirements as required by the Privacy Regulations.

### II. POLICY

The University 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 of any action, activity or designation that is required by the Privacy Regulations to be documented.

### III. PROCEDURE

1. Documentation of Privacy Policies. Written or electronic copies of the University's Privacy Policies will be maintained by the Privacy Official for at least six (6) years from the date any such Policy or Policies were created or were last in effect, whichever is later.
2. Documentation of communications required by the Privacy Regulations. Such documentation will be retained for a period of at least six (6) years from the date of creation and will be maintained in the location specified in the particular Privacy Policy in which such communication is specifically addressed. For example: The policy addressing the right of patients to have access to their protected health information (Privacy-05) states that the Access Request Form must be maintained in a patient's medical record for a minimum of six (6) years.
3. Documentation of any action, activity or designation required by Privacy Regulations. Such documentation will be retained for a period of at least six (6) years from the date of creation and will be maintained in the location specified in the particular privacy Policy in which such action, activity or designation is specifically addressed. 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 Privacy Official, in written or electronic format, for at least six (6) years.

#### **IV. REFERENCES**

1. AMC HIPAA Privacy Guidelines, PRIV. 59 (pg. 211-212).
2. HIPAA Privacy Regulations, 65 Fed. Reg. 82563, 82748–50 (December 28, 2000).

# UNIVERSITY OF OKLAHOMA

## HIPAA Privacy Policies

<b>Subject:</b> Non-Retaliation	<b>Coverage:</b> Health Care Components
<b>Policy #:</b> Privacy-13 (Admin.)	<b>Page:</b> 1 of 2
<b>HIPAA Section:</b> 164.530(g)	<b>Approved:</b> October 8, 2002
<b>Effective Date:</b> April 1, 2003	<b>Revised:</b>

### I. PURPOSE

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

### II. POLICY

Neither the University, its Health Care Components, or University Personnel, will intimidate, threaten, coerce, discriminate against, or take other retaliatory action against:

1. Individuals. Any individual for the exercise by the individual of any right under, or for participation by the individual in any process established by the Privacy Regulations;
2. Individuals and Others. Any individual or other person for:
  - a. Filing a complaint with the Secretary of the Department of Health and Human Services as permitted by the Privacy Regulations;
  - b. Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing conducted by a government enforcement agency; or
  - c. Opposing any act or practice made unlawful by the Privacy Regulations, provided the individual or person 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 "person" 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**

1. Any person who believes that some form of retaliation is occurring, or has occurred, should report the incident to the Privacy Official.
2. If the Privacy Official receives a report of retaliation or intimidation, the Privacy Official will conduct an investigation to determine if retaliation has occurred. If the report is substantiated, sanctions will be imposed.

### **IV. REFERENCES**

1. AMC HIPAA Privacy Guidelines, PRIV. 55 (pg. 204-205).
2. HIPAA Privacy Regulations, 65 Fed. Reg. 82563, 82748 (December 28, 2000).

# UNIVERSITY OF OKLAHOMA

## HIPAA Privacy Policies

<b>Subject:</b> Mitigation	<b>Coverage:</b> Health Care Components
<b>Policy #:</b> Privacy-14 (Admin.)	<b>Page:</b> 1 of 2
<b>HIPAA Section:</b> 164.530(f)	<b>Approved:</b> October 8, 2002
<b>Effective Date:</b> April 1, 2003	<b>Revised:</b>

### I. PURPOSE

To establish procedures regarding the mitigation of harmful effects of inappropriate disclosures of 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 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

1. Health Care Components must take all practicable steps to mitigate the harmful effects of a confirmed inappropriate use or disclosure. The type of mitigation that occurs will be based on the facts and circumstances of each case based on the following factors:
  - a. knowledge of where the information has been disclosed;
  - b. how the information might be used to cause harm to the patient or another individual; and
  - c. what steps can actually have a mitigating effect under the facts and circumstances of any specific situation.
2. Health Care Components must investigate the cause of the inappropriate use and/or disclosure and take corrective actions to prevent such uses and/or disclosures from re-occurring.
3. Health Care Components should notify the Privacy Official of inappropriate uses and disclosures, the mitigation efforts and the results of the investigation. The Privacy Official will

assist with the investigation and provide advice regarding mitigation efforts if requested to do so. If legal action is threatened, or is a distinct possibility, Legal Counsel must be notified.

#### **IV. REFERENCES**

1. AMC HIPAA Privacy Guidelines, PRIV. 54 (pg. 202-203).
2. HIPAA Privacy Regulations, 65 Fed. Reg. 82562-63, 82747-48 (December 28, 2000).

# UNIVERSITY OF OKLAHOMA

## HIPAA Privacy Policies

<b>Subject:</b> Amendment of Privacy Practices and Policies	<b>Coverage:</b> Health Care Components
<b>Policy #:</b> Privacy-15 (Admin.)	<b>Page:</b> 1 of 2
<b>HIPAA Section:</b> 164.530(i)(2)	<b>Approved:</b> October 8, 2002
<b>Effective Date:</b> April 1, 2003	<b>Revised:</b>

### I. PURPOSE

To outline the requirements for changes to the University's Notice of Privacy Practices and amendment of its Privacy Policies.

### II. POLICY

The University will promptly change its privacy practices and amend its Privacy Policies 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.

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 prior to the effective date of the amendment.

### III. PROCEDURE

1. Changes to Privacy Practices and Policies Addressed in the Notice of Privacy Practices.  
In order to effectuate changes to privacy practices and policies addressed in the Notice of Privacy Practices, the University will:
  - a. 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.
  - b. Document the revised Privacy Policy, in written or electronic format, and retain such documentation for at least six (6) years.
  - c. Revise the University's Notice of Privacy Practices as required by § 164.520(b)(3) of the Privacy Regulations to state the changed practice and make the revised Notice available as required by § 164.520(c) and Privacy-03. The

University may not implement an amendment to a Privacy Policy addressed in the Notice of Privacy Practices prior to the effective date of the revised Notice.

2. 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 effectuate such an amendment, the University will:
  - a. Ensure that the Privacy Policy, as amended, complies with the Privacy Regulations; and
  - b. Document the revised Privacy Policy, in written or electronic format, and retain such documentation for at least six (6) years.

#### **IV. REFERENCES:**

1. AMC HIPAA Privacy Guidelines, PRIV. 58 (pg. 208-210).
2. HIPAA Privacy Regulations, 65 Fed. Reg. 82748-82750 (December 28, 2000).

# UNIVERSITY OF OKLAHOMA

## HIPAA Privacy Policies

<b>Subject:</b> Waiver of Rights	<b>Coverage:</b> Health Care Components
<b>Policy #:</b> Privacy-16 (Admin.)	<b>Page:</b> 1 of 1
<b>HIPAA Section:</b> 164.530(h)	<b>Approved:</b> October 8, 2002
<b>Effective Date:</b> April 1, 2003	<b>Revised:</b>

### 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.

### III. PROCEDURE

1. Any person with knowledge of a violation of this policy should report the incident to the Privacy Official.
2. If the Privacy Official receives a report of a violation of this policy, the 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

1. AMC HIPAA Privacy Guidelines, PRIV. 56 (pg. 206).
2. HIPAA Privacy Regulations, 65 Fed. Reg. 82563, 82748 (December 28, 2000).

# UNIVERSITY OF OKLAHOMA

## HIPAA Privacy Policies

<b>Subject:</b> Training - Privacy	<b>Coverage:</b> Health Care Components
<b>Policy #:</b> Privacy-17 (Admin.)	<b>Page:</b> 1 of 2
<b>HIPAA Section:</b> 164.530	<b>Approved:</b> 7-1-2009
<b>Effective Date:</b> 7-1-2009	<b>Revised</b> 7-1-2009

### I. PURPOSE

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

### II. POLICY

The University will train University personnel associated with its Health Care Components regarding the Privacy Policies and the manner in which such Policies relate to the individuals' function within the University. On the Health Sciences Center campus, those individuals are all employees, students, and volunteers. On the Norman Campus, those individuals are all employees, students, and volunteers in a designated Health Care Component. Health Care Components may rely on annual training regarding the Privacy Regulations that volunteer faculty receive from another Covered Entity as long as the volunteer faculty provides evidence of such training. Volunteers other than volunteer faculty must complete the University's training, regardless of prior training.

### III. PROCEDURE

1. 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.
2. 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 and Procedure in order for the training requirement to be satisfied.
3. It is the responsibility of each Health Care Component/department, in coordination with the Privacy Official and/or Human Resources Office, to ensure that its employees, volunteers, and students receive training according to the University's HIPAA Privacy Policies.
4. A Privacy Training Coordinator, or Coordinators, should be designated by each Health

Care Component/department to coordinate with the Privacy Official and/or Human Resources Office to ensure that training is accomplished according to the University's HIPAA Privacy Policies.

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

6. Each new employee, volunteer who will provide four or more days of service, and student must complete HIPAA Privacy training within 30 days after becoming an employee, volunteer, or student. The failure of an employee, volunteer, or student to complete the required training within 30 days of becoming an employee, volunteer, or student is grounds for sanctions, up to and including termination or dismissal.

7. The University's HIPAA Privacy training is recommended for, but not required of, volunteers providing service to the University for three (3) days or fewer.

8. Effective July 1, 2009, all employees, volunteers and students at the Health Sciences Center must take the University's Privacy training annually, and those in a Health Care Component on the Norman Campus must take the Privacy training annually.

9. All volunteers, excluding volunteer faculty, are required to execute the University's Confidentiality Agreement (see the University's HIPAA Privacy Forms on the Office of Compliance website). The Health Care Component/department shall maintain that Agreement for at least six (6) years, or for as long as required by other applicable University policies.

10. Each employee, volunteer, or student whose job or academic functions are affected by a material change in the University's Privacy Policies should receive training regarding that material change within a reasonable period of time after the change becomes effective.

11. 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 re-enroll. Volunteers, including volunteer faculty, who fail to complete training or provide evidence of training, whichever is applicable, will not be permitted to provide volunteer services to the University.

12. Documentation regarding training must be maintained by the Health Care Component/department and the Privacy Official, in written or electronic format, for at least six (6) years, or for as long as required by other applicable University policies.

#### **IV. REFERENCES**

1. AMC HIPAA Privacy Guidelines, PRIV.50 (pg. 194-195)
2. HIPAA Privacy Regulations, 45 CFR §164.530.

**UNIVERSITY OF OKLAHOMA**

**HIPAA Privacy Policies**

<b>Subject:</b> Safeguards	<b>Coverage:</b> Health Care Components
<b>Policy #:</b> Privacy-18 (Admin.)	<b>Page:</b> 1 of 6
<b>HIPAA Section:</b> 164.530	<b>Approved:</b> 8/4/2008
<b>Effective Date:</b> 8/5/2008	<b>Revised:</b> 2/19/2009

**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 safeguard protected health information (PHI) from any intentional or unintentional use or disclosure in violation of the University's Privacy Policies and/or the Privacy Regulations.

**University personnel must reasonably safeguard PHI to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.**

**Health Care Components may not disclose PHI to other components of the University that are not designated Health Care Components without patient authorization or as permitted 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 and must use their best efforts to segregate the use of the PHI.**

This policy establishes minimum administrative and physical standards regarding the protection of PHI that each Health Care Component must enforce, as applicable. Health Care Components may develop additional policies and procedures that are stricter than the parameters set forth in this policy to address the unique circumstances of a particular Health Care Component. The development and implementation of policies and procedures in addition to those stated herein must be approved by the University's Privacy and Security Officials.

**Technical safeguards regarding the protection of PHI maintained in electronic form are available from the University HIPAA Security Official. They are incorporated into this Policy by reference.**

1. Administrative Safeguards.

Oral Communications. University personnel must exercise due care to avoid unnecessary disclosures of PHI through oral communications. Voices should be modulated and attention should be paid to unauthorized listeners in order to avoid unnecessary disclosures of PHI. Patient identifying information should be disclosed only during oral conversations when necessary to further treatment, payment, teaching, research or operational purposes. Dictation and telephone conversations must be conducted away from public areas if possible. Speakerphones may be used only in private areas.

Telephone Messages. Telephone messages and appointment reminders may be left on answering machines and voice mail systems, unless the patient has requested and received an alternative means of communication pursuant to Privacy-07, Communication by Alternative Means. However, each provider and/or clinic shall limit the PHI that is disclosed in a telephone message. Telephone messages regarding test results or that contain information that links a patient's name to a particular medical condition must be avoided.

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

- Only the PHI necessary to meet the requester's needs may be faxed.
- Each Health Care Component should designate employees who can fax, or approve the faxing of, PHI. Unauthorized employees, students and volunteers shall not fax PHI.
- Unless otherwise permitted or required by law, a properly completed and signed authorization must be obtained before releasing 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 as provided in Privacy-23, Authorization. PHI may be faxed to an individual if the individual requests access to his/her own PHI in accordance with Privacy-05, Patient Access to PHI.
- All faxes containing PHI must be accompanied by a cover sheet that includes a confidentiality notice. A sample fax cover sheet is attached hereto as Form-18.
- Reasonable efforts shall be made to verify that fax transmissions are sent to the correct destination. Frequently used numbers should be programmed into fax machines or computers to avoid misdialing errors. Programmed numbers should be verified on a regular basis. The numbers of new recipients should be verified prior to transmission.

- Fax machines must be located in secure areas not readily accessible to visitors or patients. Incoming faxes containing PHI must not be left sitting on or near the machine for extended periods of time.
- Fax confirmation sheets shall be reviewed to ensure the intended destination matches the number on the confirmation. The confirmation sheet shall be attached to the document that was faxed.
- All instances of misdirected faxes containing PHI must be investigated and mitigated pursuant to Privacy-14, Mitigation and Privacy-06, Accounting of Disclosures and Health Care Component reporting requirements.

Mail. PHI shall be mailed within the University in sealed envelopes. PHI mailed outside the University should be sent via first class mail and should be concealed. Appointment reminders may be mailed to a patient, unless the patient has requested and received an alternative means of communication pursuant to Privacy-07, Communication by Alternative Means.

Copying. All copies 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 certain records were acquired or disclosed.**

Sign-in Sheets. Sign-in sheets in Health Care Components, departments, or clinics that primarily see and treat patients with mental health, substance abuse, communicable disease, or other particularly sensitive conditions must structure the sign-in sheets in a manner so that subsequent signers cannot identify previous signers.

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 shredded so that it cannot be read or reconstructed. Magnetic media and diskettes containing PHI shall be overwritten or reformatted pursuant to the University Electronic Data Disposal and Reuse policy.

## 2. Physical Safeguards.

Paper Records. Paper records and medical charts 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. Paper records and medical charts on desks, counters or nurses stations must be placed face down or concealed to avoid access by unauthorized persons. Paper records shall be secured when the office is unattended by persons authorized to have access to paper records.

Original paper records and medical charts should not be removed from University premises unless necessary to provide care or treatment to a patient or required by law. University

employees shall not remove paper records or medical charts for their own convenience. Any paper records and medical charts that must be removed from University premises shall be checked out according to any applicable Health Care Component policies and procedures and must be returned as quickly as possible. The safety and return of the medical records checked out or removed are the sole responsibility of the person who checked them out or removed them.

Paper records and medical charts that are removed from University premises must not be left unattended in places in which unauthorized persons can gain access. Paper records and medical charts must not be left in unlocked automobiles or in view of passers-by.

The theft or loss of any paper record or medical chart shall be reported immediately to the Privacy Official and any person designated by the Health Care Component so that mitigation options can be considered.

Escorting Visitors and Patients. Visitors and patients must be appropriately monitored when on University premises where PHI is located to ensure they do not access PHI about other patients.

**Persons, including but not limited to pharmaceutical representatives and device salespeople, who are not employed by the University shall not be in areas in which patients are being seen or treated or where PHI is stored, without appropriate supervision.**

Computer/Work Stations. Computer monitors must be positioned away from common areas, or a privacy screen must be installed to prevent unauthorized access or observation. The screens on unattended computers must be returned to a password protected screen saver or login screen.

### 3. Technical Safeguards.

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.

E-mail within the University. Sending e-mails within the University e-mail system that contain PHI for treatment, payment, or health care operations is acceptable. PHI sent must be limited to the minimum necessary and should be sent as a limited data set when possible.

E-mail between OUHSC.EDU and HCAHealthcare.com E-mail Addresses. Sending e-mails between OUHSC.EDU and HCAHealthcare.com e-mail addresses that contain PHI for treatment, payment, or health care operations is acceptable. PHI sent must be limited to the minimum necessary and should be sent as a limited data set when possible.

E-mail Outside the University. Except in emergency situations, 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.

**All e-mails transmitted by Health Care Components or representatives thereof must contain a Confidentiality Notice similar to the following:**

**Confidentiality Notice**

This e-mail, including any attachments, contains information from 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.

**Without encryption capabilities**, if a patient sends an e-mail to a University employee, student, or volunteer asking a health care question or requesting any type of health information that would require a disclosure of PHI, the employee shall decline to respond by sending a message similar to the following:

**E-Mail Communication Denial**

“I [we] have received your health care question or request for health information. However, I [we] cannot respond using e-mail because to do so would require the transmission of information that I [we] consider to be highly sensitive and e-mails can be intercepted rather easily. We will respond to your question or request through some other means of communication. If you wish to receive health information via email, please submit the Consent for Electronic Communication form located at \_\_\_\_\_.”

**When e-mail encryption is available**, employees may send PHI only if

- 1) The patient has submitted a complete Consent for Electronic Communication Form
- 2) The email will be included in the patient’s medical record when appropriate.
- 3) The PHI will be sent, maintained, and accessed in compliance with University HIPAA policies and any Health Care Component procedures.

**Electronic Documents**. Documents and attachments and/or images containing PHI must be stored on network servers with appropriate security restrictions.

**Portable Computing Devices (i.e., laptops and hand-held computers)**. Employees, volunteer, 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 but rather should be stored on servers in a secure enterprise data center. Portable Computing Devices must never be left unattended in unsecured places. Employees storing PHI on personal

portable devices are responsible for the security of the PHI stored on such devices. PHI contained on such devices 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 employee, volunteer faculty, or student to sanctions. Volunteers, except for volunteer faculty, must never store PHI on portable devices.

Other Uses of the Internet. Any other electronic transmission of PHI requires that appropriate safeguards and procedures be implemented and approved by the Privacy and Security Officials.

The theft or loss of any electronic medical record shall be reported immediately to the Privacy and Security Officials and any person designated by the Health Care Component so that mitigation and reporting options can be considered.

### **III. REFERENCES**

1. AMC HIPAA Privacy Guidelines, PRIV. 510 (pg. 196-197).
2. HIPAA Privacy Regulations, 45 CFR §164.530.

# UNIVERSITY OF OKLAHOMA

## HIPAA Privacy Policies

<b>Subject:</b> Sanctions	<b>Coverage:</b> Health Care Components
<b>Policy #:</b> Privacy-19 (Admin.)	<b>Page:</b> 1 of 2
<b>HIPAA Section:</b> 164.530(e)	<b>Approved:</b> October 8, 2002
<b>Effective Date:</b> April 1, 2003	<b>Revised:</b>

### I. PURPOSE

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

### II. POLICY

The University will apply appropriate sanctions against University Personnel and its business associates who fail to comply with the University's Privacy Policies and/or the Privacy Regulations.

The University will not impose sanctions against University Personnel or business associate for: (a) engaging in whistleblower activities; (b) submitting a complaint to the Secretary of the Department of Health and Human Services; (c) participating in an investigation; or (d) registering opposition to a violation of the Privacy Regulations.

### III. PROCEDURE

1. Employees. A violation of the University's Privacy Policies by an employee also will be considered a violation of the University's Compliance and Quality Improvement Program (the "Program"). See, Section 6.07 of the Program. Therefore, the sanctions set forth in Section 7.03 of the Program, titled Corrective Action, will apply equally to violations of the University's Privacy Policies. The sanction imposed for a violation of the Privacy Policies will depend on the severity of the violation and will be imposed in accordance with the University's Positive Discipline Policy, or the Faculty Handbook, whichever is applicable. See, Section 3.2 of the Faculty Handbook.

2. Students. Students who violate the University's Privacy Policies will be subject to sanctions, which may include, but are not limited to: fines, suspension or expulsion. The type of sanction imposed will depend on the severity of the violation. Sanctions will be imposed on students in accordance with applicable University policies and procedures.

3. Volunteers. Volunteers who materially violate the University's Privacy Policies will not be permitted to provide further assistance to the University as a volunteer.
4. 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 his/her/its contract with the University, the University will take reasonable steps to cure the breach or end the violation, as applicable, and, if such steps are unsuccessful: (a) terminate the contract, if feasible; or (b) report the problem to the Secretary of the Department of Health and Human Services or other applicable government agency.
5. Documentation regarding any sanction imposed for a violation of the Privacy Policies should 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 be forwarded to the Privacy Official who also should maintain such documentation for the minimum retention period. Documentation of any sanction imposed against a business associate should be retained by the Privacy Official for the minimum retention period.
6. When imposing sanctions for the inappropriate use and disclosure of protected health information, consideration should be given to whether the use or disclosure was made as a result of (a) carelessness or negligence, (b) curiosity or concern, or (c) the desire for personal gain or malice.

#### **IV. REFERENCES**

1. AMC HIPAA Privacy Guidelines, PRIV. 53 (pg. 200-201).
2. HIPAA Privacy Regulations, 65 Fed. Reg. 82562, 82747 (December 28, 2000).

# UNIVERSITY OF OKLAHOMA

## HIPAA Privacy Policies

<b>Subject:</b> Uses and Disclosures - General	<b>Coverage:</b> Health Care Components
<b>Policy #:</b> Privacy-20 (Uses & Disclosures)	<b>Page:</b> 1 of 1
<b>HIPAA Section:</b> 164.502	<b>Approved:</b> October 8, 2002
<b>Effective Date:</b> April 1, 2003	<b>Revised:</b>

### I. PURPOSE

To set forth outline of required and permitted uses and disclosures.

### II. POLICY

The University cannot use or disclose protected health information, except as permitted by the Privacy Regulations and these Policies.

#### 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.

#### Permitted Uses and Disclosures

The University, and University Personnel, are permitted to use or disclose protected health information as follows: (a) for treatment, payment or health care operations, as permitted by and in compliance with Privacy-22, Treatment, Payment and Health Care Operations; (b) incident to a use or disclosure otherwise permitted or required by the Privacy Regulations as long as the minimum necessary (Privacy-21) and safeguard (Privacy-18) policies have been followed; (c) pursuant to an authorization as permitted by Privacy-23, Authorization and Privacy-28, Marketing; (d) pursuant 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 (e) as permitted by and in compliance with Privacy-24, Mental Health Records; Privacy-25, Required by Law; Privacy-27, Business Associate; Privacy-29, Fundraising; Privacy-30, Research; and Privacy-31, Limited Data Set.

# UNIVERSITY OF OKLAHOMA

## HIPAA Privacy Policies

<b>Subject:</b> Minimum Necessary Rule	<b>Coverage:</b> Health Care Components
<b>Policy #:</b> Privacy-21 (Uses & Disclosures)	<b>Page:</b> 1 of 3
<b>HIPAA Section:</b> 164.502(b) and 164.514(d)	<b>Approved:</b> October 8, 2002
<b>Effective Date:</b> April 1, 2003	<b>Revised:</b>

### I. PURPOSE

To describe the application of the minimum necessary rule to uses, disclosure and requests for protected health information.

### II. POLICY

University Personnel must make reasonable efforts to limit the Use, Disclosure of, and requests for protected health information to the minimum 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. Uses or Disclosures made to the patient or his/her legal representative (See, Privacy-02, Personal Representatives, or 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;
- e. Uses and Disclosures required by law (See, Privacy-25, Required by Law);
- f. Uses and Disclosures required by compliance with HIPAA standardized transactions.

**University Personnel may not use, disclose or request an entire medical record, except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose for the use, disclosure, or request.**

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.

### III. PROCEDURE

1. The Role Based Access Worksheet, attached hereto as Form-21, must be completed for each employee and volunteer. The Health Care Component in which the employee works will be responsible for completing the Worksheet. A copy of the Worksheet must be sent to Human Resources for inclusion in the employees file. The original should be maintained by the Health Care Component.

**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. University Personnel who are not directly involved in a patient's treatment may not have unlimited access to a 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 protected health information of patients with whom the provider has no treatment relationship, unless for research purposes as permitted by the Privacy Regulations and these Policies.**

2. The access granted to students must be determined on a case-by-case circumstance depending on the educational activity. A student's access must be determined by, and monitored by, the instructor.

#### Disclosures

3. 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 should be forwarded to the Privacy Official.

4. Non-Routine Disclosures: All non-routine disclosures (those that do not occur on a day-to-day basis as part of treatment, payment or health care operation activities or which are required by law on a regular basis) must be reviewed by Legal Counsel. When considering non-routine disclosures, Legal Counsel should consider 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 relevancy 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 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 professional or business associate represents that the information is the minimum necessary for the stated purpose(s); or (d) documentation submitted by a researcher that the information is preparatory to research, related to research on a decedent, or the disclosure has been approved by the IRB or Privacy Board.**

## **Requests**

5. 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 forwarded to the Privacy Official.
  
6. Non-Routine Requests: Each Health Care Component must designate 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). Any questions regarding the propriety of a particular request must be submitted to Legal Counsel. When considering non-routine disclosures, 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 request; (c) the relevancy of the information requested; and (d) other applicable state and federal laws and regulations.

## **IV. REFERENCES**

1. AMC HIPAA Privacy Guidelines, PRIV. 39 (pg. 154).
  
2. HIPAA Privacy Regulations, 65 Fed. Reg. 82712-82716 (December 28, 2000) and 67 Fed. Reg. 53195-53199 (August 14, 2002).

# UNIVERSITY OF OKLAHOMA

## HIPAA Privacy Policies

<b>Subject:</b> Treatment, Payment and Health Care Operations	<b>Coverage:</b> Health Care Components
<b>Policy #:</b> Privacy-22 (Uses & Disclosures)	<b>Page:</b> 1 of 2
<b>HIPAA Section:</b> 164.506	<b>Approved:</b> October 8, 2002
<b>Effective Date:</b> April 1, 2003	<b>Revised:</b>

### I. PURPOSE

To establish consent requirements and permitted uses and disclosures for treatment, payment and health care operations.

### II. POLICY

Due to ambiguities regarding consent requirements under state law and the Federal Education Rights Privacy Act (“FERPA”) which pertains to student records, Health Care Components must include language consenting to the use of a patient’s protected health information for treatment, payment and health care operations purposes with the acknowledgement of receipt of the University’s Notice of Privacy Practices. **The recommended consent language is set forth in Privacy-04, Notice of Privacy Practices.**

Health Care Components may use or disclose protected health information for their own treatment, payment or health care operations.

Health Care Components may disclose protected health information:

- a. for treatment activities of another health care provider;
- b. to another covered entity or a health care provider for the payment activities of the entity that receives the information; and
- c. 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, the health 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 of 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 of non-health care professionals; and (10) accreditation, certification, licensing or credentialing activities.**

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.

For uses and disclosures of a patient's protected health information other than for treatment, payment activities and health care operations of a Health Care Component or another health care provider, an authorization of the patient pursuant to Privacy-23 must be obtained unless disclosure pursuant to another Policy is permitted and/or required.

**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.**

### **III. REFERENCES**

1. HIPAA Privacy Regulations, 67 Fed. Reg. 53208-53219 (August 14, 2002).

# UNIVERSITY OF OKLAHOMA

## HIPAA Privacy Policies

<b>Subject:</b> Authorization	<b>Coverage:</b> Health Care Components
<b>Policy #:</b> Privacy-23 (Uses & Disclosures)	<b>Page:</b> 1 of 3
<b>HIPAA Section:</b> 164.508	<b>Approved:</b> October 8, 2002
<b>Effective Date:</b> April 1, 2003	<b>Revised:</b>

### I. PURPOSE

To establish authorization requirements for uses and disclosures 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 treatments, payment and health care operations, without a valid written authorization from the patient, except as otherwise permitted by these Policies. When a Health Care Component obtains or receives a valid authorization for its use or disclosure of protected health information, such use or disclosure must be consistent with the authorization.

Information released pursuant to this 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.

**An authorization is required to disclose information to third parties for purposes other than treatment, payment or health care operations and for use by or disclosures to departments 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 certain circumstances. See, Privacy-24, Mental Health Records.

#### 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 provision of an authorization, except in the context of research involving treatment. See, Privacy-30, Research.

**One exception to the prohibition on conditioning authorization relates to health care services provided at the request of a third party. For example, Health Care Components can require an authorization as a condition to providing a drug screening test or physical requested by an employer.**

## Revocation of Authorizations

Health Care Components must permit patients to revoke their authorizations, except to the extent the Health Care Component has taken action in reliance on the authorization.

## III. PROCEDURES

1. A valid authorization must contain all of the elements required by the Privacy Regulations. A sample authorization form is attached hereto as Form-23.
2. Prior to using or disclosing protected health information pursuant to an authorization, University Personnel must review the authorization to determine if it is valid. An authorization is not valid, if it contains any of the following defects:
  - a. the expiration date has passed or the expiration event is known to have occurred;
  - b. the authorization has not been filled out completely,
  - c. University Personnel have knowledge that the authorization has been revoked;
  - d. University Personnel have knowledge that some material information in the authorization is false;
  - e. the authorization was obtained by improperly conditioning treatment upon its receipt; or
  - f. if the authorization is for psychotherapy notes, it is improperly combined with another type of authorization or document.
3. 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.
4. Health Care Components must keep copies of authorizations for at least six (6) years.

#### **IV. REFERENCES**

1. AMC HIPAA Privacy Guidelines, PRIV. 10 (pg. 90)
2. HIPAA Privacy Regulations, 65 Fed. Reg. 82650-82662 (December 28, 2000) and 67 Fed. Reg. 53219-53226
3. 42 C.F.R. § 2.31.

# UNIVERSITY OF OKLAHOMA

## HIPAA Privacy Policies

<b>Subject:</b> Mental Health Records	<b>Coverage:</b> Health Care Components
<b>Policy #:</b> Privacy-24 (Uses & Disclosures)	<b>Page:</b> 1 of 2
<b>HIPAA Section:</b> 164.508	<b>Approved:</b> October 8, 2002
<b>Effective Date:</b> April 1, 2003	<b>Revised:</b>

### I. PURPOSE

To establish permitted uses and disclosures of mental health records, including psychotherapy notes.

### II. POLICY

#### 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 set forth in Privacy-01, number 29. 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.

Persons or entities not covered by the Privacy Regulations 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.

**An authorization for the use or disclosure of psychotherapy notes cannot be combined with another authorization.**

## Psychotherapy Notes

A patient does not have a right to access psychotherapy notes relating to him/herself except (i) to the extent 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;
3. Use or disclosure to Legal Counsel to defend the University in a legal action or other proceeding brought by the patient;
4. Use or disclosure of psychotherapy notes 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 other duties as authorized by law; 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 health plan 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

1. HIPAA Privacy Regulations, 65 Fed. Reg. 82652-82655 (December 28, 2000) and 67 Fed. Reg. (August 14, 2002).

# UNIVERSITY OF OKLAHOMA

## HIPAA Privacy Policies

<b>Subject:</b> Required by Law	<b>Coverage:</b> Health Care Components
<b>Policy #:</b> Privacy-25 (Uses & Disclosures)	<b>Page:</b> Page 1 of 11
<b>HIPAA Section:</b> 164.510(a)	<b>Approved:</b> October 8, 2002
<b>Effective Date:</b> April 1, 2003	<b>Revised:</b> March 1, 2003

### I. PURPOSE

To set forth requirements pertaining to uses and disclosures required by law.

### II. POLICY

University Personnel may disclose protected health information without the patient's consent, authorization or the 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 must be submitted to Legal Counsel.**

### III. PROCEDURE

1. Abuse or Neglect of Children.

a. Reporting Child Abuse, Neglect or the Birth of a Chemically Dependent Child.

All University Personnel who have reason to believe that a child under the age of 18 is a victim of abuse or neglect or who attends the birth of a child who tests positive for alcohol or a controlled dangerous substance must promptly notify the Oklahoma Department of Human Services. Health Care Components may establish procedures for facilitating and coordinating reporting requirements.

“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.

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

Reports of abuse or neglect may be made by telephone, in writing, or in person. 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.

Health Care Components must also 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 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.

b. 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 or 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 may establish procedures for facilitating and coordinating reporting requirements.

c. Notification. To the extent a report is made pursuant to this provision, 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, believes 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.

2. Adult Victims of Abuse, Neglect, Domestic Violence or Criminally Injurious Conduct.

a. 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 either 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 Oklahoma City Police Department or sheriff's department.

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 or 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 or herself from abuse, neglect, or exploitation without assistance from others.

"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.

"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.

"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.

The report 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.

b. Reporting Criminally Inflicted Injuries. Any University Personnel examining, attending, or treating a patient of 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 may establish procedures for facilitating and coordinating reporting requirements.

c. Notification. To the extent a report is made pursuant to this provision, 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, believes 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 Vulnerable Adult.

3. Court Orders. A court order is a direction of the court which directs a party to produce certain specified documents. Upon the receipt of a court order requesting the disclosure of medical records containing protected health information and meeting all legal requirements, University Personnel or the recipient of the order must immediately forward the court order to the University's Legal Counsel. Upon determining that the court order is valid and meets all legal requirements, the University should release the information pursuant to the court order. The patient whose records are being requested is not required to provide an authorization to disclose 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, which is conducted, regulated by, or assisted by any United States department or agency, shall be confidential.

The content of these records may be disclosed to third parties as follows: (i) in accordance with the patient's prior written consent; (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. Part 2.

4. Subpoenas. 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.

**Upon receipt of a subpoena, University Personnel or the recipient of the subpoena must immediately forward the subpoena to Legal Counsel to determine if PHI can be released pursuant to the subpoena. See Form-25, Requirements for Content and Service of a Subpoena.**

5. Other Disclosures to Law Enforcement Officials.

a. Certain limited protected health information may be disclosed regarding a patient 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. A “law enforcement official” means an officer or employee of any agency or authority of the United States, State, Indian tribe, county, city, town or municipality, 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.

If a request is made by a law enforcement official for a patient’s protected health information, Legal Counsel shall be immediately contacted to authenticate the request for disclosure and to determine whether the official is authorized to make such a request. Upon determining if the request is valid, Legal Counsel shall direct the appropriate person(s) to provide the limited information set forth below.

The disclosure of protected health insurance pursuant to this section, is limited only 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.

**Do 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.**

b. 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 possible; and (iii) de-identified information cannot be reasonably used. University Personnel should consult with Legal Counsel before making any disclosures pursuant to this provision.

c. In addition to other disclosures regarding potential victims of a crime discussed in this policy, the University may disclose to law enforcement officials information about a patient who 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, all of the following requirements are met: (a) the law enforcement official represents that such information is needed to determine whether a violation of law by a person other than the patient has occurred, and such information is not intended to be used against the patient and 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) the disclosure is in the best interest of the patient as determined by University Personnel, in the exercise of professional judgment. University Personnel should consult with Legal Counsel before making any disclosures pursuant to this provision.

d. The University may disclose to a law enforcement official PHI that University Personnel believe in good faith constitutes evidence of criminal conduct that occurred on University property. University Personnel should consult with Legal Counsel before making any disclosures pursuant to this provision.

e. University Personnel providing emergency health care in response to a medical emergency, other than an emergency on University property, 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 Legal Counsel before making any disclosures pursuant to this provision.

6. Uses or Disclosures to Avert Serious 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 authorities 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. Legal Counsel should be consulted before any disclosures of PHI are made pursuant to this Section.

7. Uses and Disclosures for Special Government Functions.

a. The University may use and disclose protected health information of patients in the United States and foreign armed forces for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission. Legal Counsel should be consulted to confirm that the requirements of this disclosure are met.

b. 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. Legal Counsel should be consulted to confirm that the requirements of this disclosure are met.

c. 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) the provision of health care to such individuals; (ii) the health and safety of such individual or other inmates; (iii) 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) law enforcement on the premises of the correctional institution; and/or (v) the administration and maintenance of the safety, security, and good order of the correctional institution. Legal Counsel should be consulted to confirm that the requirements of this disclosure are met.

8. Public Health. University Personnel may disclose protected health information without the written authorization of the patient to the appropriate state or federal health authority conducting public health surveillance, public health investigations, public health interventions and the Food and Drug Administration regulatory oversight. Such permitted disclosures shall specifically include the following:

a. 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. This includes discharge data including, but not limited to, complete discharge data sets or comparable information for each patient discharged.

Legal Counsel must 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 which is specified in the request.

b. 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.

This 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.

c. Death Certificates. A death certificate for each death which 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 or the medical examiner at the University who was responsible for the patient's care. 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 alternative 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.

d. Communicable or Venereal 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" means syphilis, gonorrhea, chancroid, granuloma inguinale, lymphogranuloma venereum and any other disease which 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 is declared to be communicable and dangerous to the public health.

Protected health information relating to communicable or venereal disease may be released without patient authorization under the following limited circumstances:

1. Court Order. Release of protected health information may be made upon receipt of a court order.
2. Administrative Orders. Release of limited protected health information relating to venereal 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. Before releasing any information pursuant to this subsection, University Personnel should contact Legal Counsel for a determination of the validity of the order.

3. 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.

4. 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.

5. 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 disease of the patient whose information is released.

6. Reports of Venereal Disease. All University Personnel who make a diagnosis or treats a patient for any venereal disease, as defined above, must promptly report the case, in writing, to the State Commissioner of Health. If the University Personnel knows or has good reason to suspect that the patient having a venereal disease is conducting him or herself as to expose other persons to infection, or is about to so conduct him or herself in such a way, the 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.

e. Infant Eye Infections. University Personnel must report to the State Department of Health, any cases of ophthalmia neonatorum, or inflammation of the eyes of a newborn, occurring at any time within four (4) weeks after the infant's birth. Any University Personnel who knows that an infant has ophthalmia neonatorum must report the case within six (6) hours of the discovery to the State Department of Health and confirm the case in writing within three (3) days to the State Department of Health. This report may require disclosure of the infant's protected health information.

f. 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.

g. 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 diagnostic code categories 740 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 request.

h. 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 which is necessary to further the recognition, prevention, control, treatment and cure of cancer, precancerous and tumorous diseases.

The Commissioner may require the University to report the following information regarding cancerous, precancerous and tumorous diseases:

1. The patient's name, address, age, race, sex, social security number and hospital identifier or other identifier.
2. The patient's residential, family, environmental, occupational and medical histories; and
3. The physician's name, diagnosis, stage of the disease, method of treatment and the name and address of any facility providing treatment.

9. Medicaid Program. University Personnel must provide the Attorney General of Oklahoma access to all records of Medicaid recipients under the Oklahoma Medicaid Program which 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.

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.

10. 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, 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 which 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, 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, which 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.

11. Disclosures to Funeral Directors. The University may disclose protected health information to funeral directors as necessary 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.

12. Cadaveric Organ, Eye or Tissue Donations. University Personnel may use or disclose 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.

13. Workers' Compensation. Under the Oklahoma's Workers' Compensation laws, an employer must provide to an injured employee medical, surgical or other attendance or treatment, nurse and hospital service, medicine, crutches, and apparatus as may be necessary after an injury which occurred during the course of his 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 to the employer of the injured employee.

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 contemplated that an employee who participates in the benefits of this Act is deemed to consent to the treating physician in making these reports. Thus, the patient authorization is not required. However, uses and disclosures made under this section must be limited only to that protected health information which is relevant to the injury for which benefits are sought.

# UNIVERSITY OF OKLAHOMA

## HIPAA Privacy Policies

<b>Subject:</b> Disclosures to Family and Others Involved in Patient's Care	<b>Coverage:</b> Health Care Components
<b>Policy #:</b> Privacy-26 (Uses & Disclosures)	<b>Page:</b> 1 of 2
<b>HIPAA Section:</b> 164.510(b)	<b>Approved:</b> October 8, 2002
<b>Effective Date:</b> April 1, 2003	<b>Revised:</b>

### I. PURPOSE

To articulate conditions under which family and friends can be notified of patient's condition.

### II. POLICY

University Personnel may disclose protected health information to a patient's family member, other relative, or a close personal friend of the individual, or any other person identified by the individual, as long as the protected health information disclosed is **relevant** to the person's involvement with the patient's care or payment related to the patient's health care.

University Personnel may use or disclose protected health information 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 individual's location, general condition, or death.

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 individual's location, general condition, or death.

### III. PROCEDURES

1. Patient is Present – If the patient is present for, or otherwise available prior to, a use or disclosure to a family member or friend as described above and has the capacity to make health care decisions, University Personnel may use or disclose the protected health information if he/she:

- a. Obtains the patient's agreement and documents the agreement in the patient's medical record;
- b. 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

c. Reasonably infers from the circumstances, based on the exercise of professional judgment that the individual does not object to the disclosure.

2. **Patient is not Present** – If the patient is not present, or the opportunity to agree or object to the use of 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 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 his/her 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.**

3. 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 friend:

- a. Whether the potential disclosure is common practice;
- b. The nature of the relationship between the parties;
- c. The sensitive nature of the information being disclosed;
- d. The ability of the patient to manage necessary tasks (i.e., pick up prescriptions, medical supplies, x-rays, or other forms of protected health information); and
- e. Whether the 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.

4. University Personnel are not required to verify the relationship of relatives or other individuals involved in the patient’s care. University Personnel may simply inquire into the individual’s relationship with the patient. The patient’s act of involving the other person in his/her care also may suffice as verification of their identity.

#### **IV. REFERENCES**

- 1. AMC HIPAA Privacy Guidelines, PRIV. 23 (pg. 119).
- 2. HIPAA Privacy Regulations, 65 Fed. Reg. 82663-82666 (December 28, 2000).

# UNIVERSITY OF OKLAHOMA

## HIPAA Privacy Policies

<b>Subject:</b> Business Associates	<b>Coverage:</b> Health Care Components
<b>Policy #:</b> Privacy-27 (Uses & Disclosures)	<b>Page:</b> 1 of 2
<b>HIPAA Section:</b> 164.502(e), 164.504(e) and 164.532	<b>Approved:</b> October 8, 2002
<b>Effective Date:</b> April 1, 2003	<b>Revised:</b>

### 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 or receive protected health information on its behalf, if the Health Care Component ensures that the University has executed an agreement with the business associate which contains language requiring the business associate to appropriately safeguard the protected health information.

**A Business Associate is a person or entity who provides certain functions, activities, or services on behalf of the University, that involves the use and/or disclosure of protected health information. See the Business Associate Decision Tree attached hereto as Form-27.**

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 and/or the Health Care Component must take reasonable steps to cure the breach or end the violation. If such steps are unsuccessful, the business associate agreement must be terminated or, if termination is not possible, the problem with the Business Associate must be reported to the Secretary of the Department of Health and Human Services.

### III. PROCEDURE

1. The University's Office of Legal Counsel will be responsible for drafting and implementing the appropriate business associate language and/or agreements. All contracts must be reviewed in accordance with University policies. Questions regarding the status of a vendor or independent contract should be forwarded to Legal Counsel.

2. Health Care Components must identify Business Associates and bring the need for contractual language to the attention of Legal Counsel.

**The business associate language must be included in new or renewing contracts. The University has until April 14, 2004 to include the appropriate language into existing agreements.**

#### **IV. REFERENCES**

1. AMC HIPAA Privacy Guidelines, PRIV. 03 and .16 (pg. 70 and 108).
2. HIPAA Privacy Regulations, 65 Fed. Reg. 82475-76, 82499 (December 28, 2000) and 67 Fed. Reg. 53248-53254 and 53264-53266 (August 14, 2002).

# UNIVERSITY OF OKLAHOMA

## HIPAA Privacy Policies

<b>Subject:</b> Marketing	<b>Coverage:</b> Health Care Components
<b>Policy #:</b> Privacy-28 (Uses & Disclosures)	<b>Page:</b> 1 of 1
<b>HIPAA Section:</b> 164.508(a)(3)	<b>Approved:</b> October 8, 2002
<b>Effective Date:</b> April 1, 2003	<b>Revised:</b>

### I. PURPOSE

To establish requirements pertaining to the use and disclosure of protected health information for marketing purposes.

### II. POLICY

Health Care Components must obtain an authorization for any use or disclosure of protected health information for marketing, **except** if the communication is in the form of: (a) a face-to-face communication made by University Personnel to an individual; or (b) a promotional gift of nominal value provided by the Health Care Component. See, Privacy-23, Authorization, for the requirements of a valid authorization.

**“Marketing” does not include communications about medical services or products provided by the University or one of its Health Care Components.**

If the marketing involves direct or indirect payment to the University or a Health Care Component from a third party, the authorization must state that payment is involved.

**University Personnel are prohibited from selling patient lists to third parties, or from disclosing protected health information to a third party for the independent marketing activities of the third party, without obtaining an authorization from every patient on the list.**

### III. PROCEDURE

Authorizations for marketing should be kept in a patient’s medical record for at least six (6) years from the date it was signed.

### IV. REFERENCES

1. AMC HIPAA Privacy Guidelines, PRIV. 24 (pg. 121).
2. HIPAA Privacy Regulations, 65 Fed. Reg. (December 28, 2000) and 67 Fed. Reg. (August 14, 2002).

# UNIVERSITY OF OKLAHOMA

## HIPAA Privacy Policies

<b>Subject:</b> Fundraising	<b>Coverage:</b> Health Care Components
<b>Policy #:</b> Privacy-29 (Uses & Disclosures)	<b>Page:</b> 1 of 2
<b>HIPAA Section:</b> 164.514(f)(1)	<b>Approved:</b> October 8, 2002
<b>Effective Date:</b> April 1, 2003	<b>Revised:</b>

### I. PURPOSE

To establish requirements pertaining to the use and disclosure of protected health information for fundraising purposes.

### II. POLICY

Health Care Components may use, or disclose to a business associate or to an institutionally related foundation, the following protected health information for the purpose of raising funds for its own benefit, without an authorization: (a) demographic information relating to an individual; and (b) dates of health care provided to an individual.

**Any use or disclosure for fundraising purposes beyond demographic information requires the patient's authorization. Demographic information includes the patient's name, address, age and gender. It does not include the use or disclosure of any information about a patient's illness or treatment. See Privacy-23, Authorization, for requirements of a valid authorization. This restriction makes "grateful patient" campaigns infeasible.**

A patient's demographic information and dates of receipt of health care services may not be used or disclosed with the patient's authorization for fundraising purposes unless the following requirements are met:

1. The University's Privacy Notice must contain a statement that the University may contact the patient to raise money for the University; and
2. The Privacy Notice and all fundraising materials must describe the procedures for a patient to opt out of receiving any additional fundraising communications.

### III. PROCEDURE

1. All fundraising materials directed to patients, as well as the Notice of Privacy Practices, must indicate that a patient can opt out of receiving fundraising materials from the University, or a Business Associate or related foundation on the University's behalf, by sending a letter or e-mail to the University's Privacy Official.

2. The University's foundations and all Health Care Components must get the approval of the Privacy Official prior to initiating any fundraising campaigns directed at patients of the Health Care Components to ensure patients are not solicited who have indicated that they do not want to receive fundraising materials.

#### **IV. REFERENCES**

1. AMC HIPAA Privacy Guidelines, PRIV. 25 (pg. 123).

2. HIPAA Privacy Regulations, 65 Fed. Reg. (December 28, 2000) and 67 Fed. Reg. (August 14, 2002).

**correction 4/10/02**

**UNIVERSITY OF OKLAHOMA**

**HIPAA Privacy Policies**

<b>Subject:</b> Research	<b>Coverage:</b> Health Care Components
<b>Policy #:</b> Privacy-30 (Uses & Disclosures)	<b>Page:</b> 1 of 1
<b>HIPAA Section:</b>	<b>Approved:</b> October 8, 2002
<b>Effective Date:</b> April 1, 2003	<b>Revised:</b>

**This section is currently under development.**

# UNIVERSITY OF OKLAHOMA

## HIPAA Privacy Policies

<b>Subject:</b> Limited Data Sets	<b>Coverage:</b> Health Care Components
<b>Policy #:</b> Privacy-31 (Uses & Disclosures)	<b>Page:</b> 1 of 2
<b>HIPAA Section:</b> 164.514(e)	<b>Approved:</b> October 8, 2002
<b>Effective Date:</b> April 1, 2003	<b>Revised:</b>

### I. PURPOSE

To establish permitted uses of limited data sets 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 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 end the violation, as applicable. If such steps are unsuccessful, the Health Care Component must discontinue disclosure of protected health information to the recipient and report the problem to the Secretary of the Department of Health and Human Services.

**A limited data set is protected health information that does not directly identify the patient, but which contains certain potentially identifying information.**

### III. PROCEDURE

1. 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:

- a. Names
- b. Postal address information, other than town, city, state, and zip codes
- c. Telephone numbers
- d. Fax numbers
- e. Electronic mail addresses

- f. Social security numbers
- g. Medical record numbers
- h. Health plan beneficiary numbers
- i. Account numbers
- j. Certificate/license numbers
- k. Vehicle identifiers and serial numbers, including license plate numbers
- l. Device identifiers and serial numbers
- m. Web Universal Resource Locators (URLs)
- n. Internet Protocol (IP) address numbers
- o. Biometric identifiers, including finger and voiceprints
- p. Full-face photographs and comparable images

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

2. Data Use Agreements. All data use agreements must be approved by Legal Counsel prior to execution. A Data Use Agreement must:

- a. Establish the permitted uses and disclosures of the limited data set.
- b. Establish who is permitted to use or receive the limited data set.
- c. Provide that the recipient of the information will:
  - Not use or further disclose the information other than as permitted by the agreement
  - Use appropriate safeguards to prevent use or disclosure other than as permitted by the agreement
  - Report to the University any uses or disclosures the recipient is aware of that is not provided for by the agreement
  - Ensure that the recipient's agents who have access to the information agree to the same restrictions as imposed on the recipient
  - Not identify the information or contact the patients

#### **IV. REFERENCES**

1. HIPAA Privacy Regulations, 67 Fed. Reg. 53234, 53240 (August 14, 2002).

# UNIVERSITY OF OKLAHOMA

## HIPAA Privacy Policies

<b>Subject:</b> De-Identified Information	<b>Coverage:</b> Health Care Components
<b>Policy #:</b> Privacy-32 (Uses & Disclosures)	<b>Page:</b> 1 of 3
<b>HIPAA Section:</b> 164.502(d) & 164.514(a)&(b)	<b>Approved:</b> October 8, 2002
<b>Effective Date:</b> April 1, 2003	<b>Revised:</b>

### I. PURPOSE

To establish the method for de-identifying health information.

### II. POLICY

#### De-Identified Information

Health Care Components can use and disclose de-identified health information without regard to the policies, 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 becomes subject to regulation under the Policies.

**Health information that does not identify the patient and in which there is no reasonable basis to believe that the health information can be used to identify the patient, or “de-identified information” is not considered protected health information and is not subject to the requirements of this Policy.**

### III. PROCEDURE

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

1 Safe Harbor. The following identifiers of the patient or of the relatives, employers, or household members of the patient are removed:

- a. Names
- b. Geographic subdivision, such as street address, city, county, and zip code

- c. The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people, and if it has fewer than 20,000 the zip code 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).
- d. 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.
- e. Telephone numbers
- f. Fax Numbers
- g. E-mail addresses
- h. Social security numbers
- i. Medical record numbers
- j. Health plan beneficiary numbers
- k. Account numbers
- l. Certificate/license numbers
- m. Vehicle identifiers, serial numbers, license plate numbers
- n. Device identifiers and serial numbers
- o. Web Universal Resource Locators (URLs)
- p. Internet Protocol address numbers (IP)
- q. Biometric identifiers, including finger and voiceprints
- r. Full face photographic images and other comparable images
- s. All other unique identifying number, characteristic, or code.

2. Alternative Method of De-Identification. A biostatistician or some other 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 document the methods and results of the analysis that justify the determination.

### **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**

1. AMC HIPAA Privacy Guidelines, PRIV-15 (pg. 107).
2. HIPAA Privacy Regulations, 65 Fed. Reg. 82499 (December 28, 2000).

# UNIVERSITY OF OKLAHOMA

## HIPAA Privacy Policies

<b>Subject:</b> Facility Directory	<b>Coverage:</b> Health Care Components
<b>Policy #:</b> Privacy-33 (Uses & Disclosures)	<b>Page:</b> 1 of 2
<b>HIPAA Section:</b> 164.510(a)	<b>Approved:</b> October 8, 2002
<b>Effective Date:</b> April 1, 2003	<b>Revised:</b>

### I. PURPOSE

To establish requirements for including a patient's name in a facility directory.

### II. POLICY

Health Care Components may use or disclose certain protected health information without the written authorization of the patient for the purpose of maintaining a facility directory. The following protected health information may be used in a facility directory:

1. The patient's name.
2. The patient's location within the facility. A Health Care Component may **not** release information that indicates a patient is being treated in an area of the University that is limited to treatment of certain diseases or conditions, such as alcohol or drug rehabilitation, detoxification, psychiatric treatment, or communicable disease treatment.
3. The patient's condition described in general terms (such as stable, fair, serious) that does not communicate specific medical information.
4. The patient's religious affiliation (**may be disclosed to members of the clergy only**).

The information in a facility directory may be disclosed to any person who **asks for the patient by name**. However, a patient's religious affiliation may only be disclosed to members of the clergy.

### III. PROCEDURE

1. At the time of facility registration, patients must be informed, either orally or in writing, of the Health Care Component's intent to use or disclose certain protected health information in the facility directory. The patient must be informed of the type of

information that will be disclosed and the persons to whom the information may be disclosed.

2. If the patient indicates that he/she **does not** want to be included in the facility directory, he/she should be asked to complete the “Directory Opt-Out” form attached hereto as Form-33.

3. In an emergency situation, a Health Care Component may include the patient’s information in a facility directory if it University Personnel determine it is in the patient’s best interest. The Health Care Component must give the patient the opportunity to object to the placement in the directory as soon as it becomes practicable to do so.

#### **IV. REFERENCES**

1. AMC HIPAA Privacy Guidelines, PRIV. 22 (pg. 117).

2. HIPAA Privacy Regulations, 65 Fed. Reg. 82521, 82662-63 (December 28, 2000).

**UNIVERSITY OF OKLAHOMA**

**HIPAA Privacy Policies**

<b>Subject:</b> Breach of Unsecured PHI	<b>Coverage:</b> Health Care Components
<b>Policy:</b> Privacy 34	<b>Page:</b> 1 of 3
<b>HITECH Act Section:</b> 13402	<b>Approved:</b>
<b>Effective Date:</b> 9/22/2009	<b>Revised:</b>

**I. PURPOSE**

To provide for notification in the case of breaches of unsecured protected health information. For purposes of these requirements, section 13402(h) of the HITECH Act (“Act”) defines “unsecured protected health information” to mean protected health information that is not secured through the use of approved technologies or methodologies.

To be approved, technologies and methodologies must render protected health information unusable, unreadable, or indecipherable to unauthorized individuals.

**II. POLICY**

The University, through its Health Care Components, 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.**

This policy establishes the requirements as outlined by the Act 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. The breach notification provisions of section 13402 of the Act apply to HIPAA covered entities and their business associates that access, maintain, retain, modify, record, store, destroy, or otherwise hold, use, or disclose unsecured PHI.

Each Health Care Component shall designate an individual to be responsible for compliance with this policy, in coordination with the HIPAA Privacy and Security Officials.

1. Methods of Protection – Either of the following methods may be used to secure PHI and make it unusable, unreadable, or indecipherable to unauthorized individuals.
  - a. **Encryption** – The University and each Health Care Component will implement and maintain reasonable and appropriate encryption technologies and methodologies to enhance the protection of PHI.
    - i. Refer to University Security policies (available on the Information Technology webpage) for encryption requirements.
  - b. **Destruction** – The University and each Health Care Component will implement destruction techniques that render PHI unusable and/or unreadable in any format.
    - i. Refer to University Security policies (available on the Information Technology webpage) for destruction requirements.

**PHI secured by one of the above methods is not insecure and is therefore not subject to this policy.**

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

2. Notification of Breach
  - a. In the event a breach of unsecured PHI is discovered, the University or its designee is required to notify each individual whose unsecured PHI has been, or is reasonably believed to have been, inappropriately accessed, acquired, or disclosed, according to the requirements of the Act:
    - i. Written notice to the individual (or next of kin 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 specified by the individual);
    - ii. In the case in which there is insufficient or out-of-date contact information, substitute notice, including, in the case of 10 or more individuals for which there is insufficient contact information, conspicuous posting (for a period determined by the Secretary) on the home page of the web site of the University or notice in major print or broadcast media;
    - iii. In cases that the Health Care Component or University deem urgent based on the possibility of imminent misuse of the unsecured PHI, notice by telephone or other method is permitted in addition to the above methods.
  - b. Details of the notice shall include the following:
    - i. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
    - ii. A description of the types of unsecured PHI that were involved in the breach

(such as full name, SSN, DOB, home address, account number, or disability code);

- iii. The steps individuals should take to protect themselves from potential harm resulting from the breach;
  - iv. A brief description of what the covered entity involved is doing to investigate the breach, to mitigate losses, and to protect against any further breaches;
  - v. Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, web site, or postal address.
- c. If a breach involves more than 500 individuals, the HIPAA Privacy and Security Officials must be notified immediately. They will determine whether and when a notice to the individual, the media, and/or HHS is appropriate and, if so, the content of the notice.

### 3. Tracking

- a. Health care components must maintain a log of breaches of unsecure PHI and notify the HIPAA Privacy Official of each breach.
- b. The University, through the HIPAA 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, as required by the Act.

## **III. REFERENCES**

1. HITECH Act Section 13402 of Title XIII of the American Recovery and Reinvestment Act of 2009, (effective February 17, 2009)
2. HITECH Act Breach Notification Regulations (effective September 2009)
3. Department of Health and Human Services
4. HIPAA Privacy & Security Rules 45 CFR Parts 160, 162, and 164
5. NIST SP 800-111 "*Guide to Storage Encryption Technologies for End User Devices*" and SP 800-88 "*Guidelines for Media Sanitization*"
6. Oklahoma State Breach Notification Law, Section 298 [HB 2357], (effective June 8, 2006)
7. Oklahoma State Breach Notification Law, [HB 2245], (effective November. 1, 2008)