UNIVERSITY OF OKLAHOMA

HIPAA Policies

Title: Statement of Structure and Policy	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Last Revised:** 2/1/16; 5/5/16; 4/1/18; 1/22/19

I. POLICY*

A. Structure - The University of Oklahoma is comprised of two covered entities[1] for purposes of HIPAA compliance – the Norman campus and the Health Sciences Center campus.[2] Each campus covered entity is designated as a hybrid entity, and those parts of the campus that are subject to the University's HIPAA Compliance Program have been further designated as Health Care Components of that campus covered entity. (For specific campus designations, refer to the HIPAA Definitions policy.)

B. Policies - Each of the University's campus covered entities shall, through its Workforce Members, protect and safeguard the Protected Health Information (PHI), created, acquired, and/or maintained by its Health Care Components as required by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended, and applicable laws, through these University HIPAA Privacy and Security policies. The University's HIPAA policies shall:

1. Ensure the Confidentiality, Integrity, and Availability of all PHI that it creates, receives, maintains, or transmit electronically;
2. Protect against any reasonably anticipated threats or hazards to the security or Integrity of such information;
3. Protect against any reasonably anticipated Uses or Disclosures of such information that are not permitted or required under the HIPAA Privacy or Security rules, and
4. Reflect the University's accepted moderate operative level of risk.

The policies are also intended to provide assistance and direction to Workforce Members in regard to the protection of the privacy rights of patients by (a) establishing rules related to the Use and Disclosure of Protected Health Information; (b) affording patients and authorized individuals with access to and information regarding the Disclosure of their Protected Health Information; and (c) directing the development and implementation of procedures intended to assist patients and University Personnel with regard to HIPAA.

Policies governing the University's Health Plans[3] are maintained in the Office for Human Resources for each campus and on the HIPAA web pages. Polices governing the University human subjects research are maintained by the HRPP Office and on the HIPAA webpage.

C. Conflicting Policies - These policies supersede and replace any conflicting policies and procedures of any University campus covered entity or Health Care Component relating to the Use and

[1] Effective January 7, 2019.
[2] The Tulsa campus shall be considered part of the Health Sciences Center HIPAA Compliance Program, subject to the HSC HIPAA Privacy and Security policies, procedures, and practices.
[3] The Health Plans on each of the Norman, Health Sciences Center, and Tulsa campuses are each separate covered entities, operating under the University's HIPAA Privacy and Security policies for Health Plans.

*Capitalized terms are defined in HIPAA *Definitions* policy

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

These policies apply to all forms of Protected Health Information (oral, written, and electronic).

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

. Campus covered entities and Health Care Components are reminded that these policies must be read in conjunction with other University polices, including but not limited to IT and IT Security policies, Purchasing policies, Risk Management policies, and Record Retention policies.

In the event of conflict between a HIPAA policy and any University policy, campus covered entities and Health Care Components shall comply with the policy that provides the most protection to Protected Health Information and shall notify the HIPAA Security Officer or University Privacy Official of the conflict.

D. Exceptions – Campus covered entities and Health Care Components that believe they have unique circumstances that warrant an exception to a HIPAA Policy must contact the University Privacy Official.

II. REFERENCES

A. HIPAA Regulations - 45 CFR 164.304, 164.306
B. Campus Advisory Committee minutes, January 7, 2019

UNIVERSITY OF OKLAHOMA

HIPAA Policies

Title: Definitions – Privacy and Security	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Last Revised:** 4/18/16; 5/5/16, 4/1/18, 1/31/19

I. DEFINITIONS

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

The terms "must," "shall," "may not," and "will" are used to indicate requirements; "should" and "may" are used to indicate recommended actions.

Access. The ability or means necessary to read, write, modify, or communicate data/information or otherwise use any Information System.

Administrative Safeguards. Administrative actions, policies, and procedures designed to protect PHI and to manage the conduct of the University's Workforce Members in relation to protecting PHI.

Affiliated Covered Entity. Legally separate Covered Entities under common ownership or control. The University's Norman campus and Health Sciences Center campus, which have separate state agency numbers but common ownership and control by the University of Oklahoma President and the Board of Regents, have designated themselves as an Affiliated Covered Entity to provide for sharing of PHI. (The Tulsa campus is considered part of the Health Sciences Center campus for purpose of the HIPAA Compliance Program.)

Authentication. Corroboration that a person is who he says he is.

Authorization. The written permission from a patient to a Covered Entity or Health Care Component to Use or Disclose the patient's Protected Health Information. 45 CFR § 164.508 (c).

Availability. Meaning that data or information is accessible and usable upon demand by an authorized person.

Breach. The acquisition, Access, Use, or Disclosure of Protected Health Information in a manner not permitted under HIPAA that compromises the security or privacy of the Protected Health Information. 45 CFR § 164.402.

Business Associate. A person or entity who is not a Workforce Member and who creates, receives, maintains, or transmits Protected Health Information for a covered function or activity, for or on behalf of the University. Such activity may include, but is not limited to, billing; repricing; claims processing and administration; data analysis; legal, accounting, and actuarial services; certain patient safety activities; consulting; benefit management; practice management;

utilization review; quality assurance; and similar services or functions. A Business Associate may be a Covered Entity. 45 C.F.R. § 160.103.

Note: The University may also serve as a Business Associate of another Covered Entity, as described in HIPAA *Business Associates* policy.

Confidentiality. Meaning that data or information is not to be made available or disclosed to unauthorized persons or entities.

Control. A safeguard or countermeasure. Controls include practices, policies, procedures, programs, techniques, guidelines, organizational structures, and the like.

Control Review. A part of the risk management process that compares existing controls for data and/or information resources with respect to defined security requirements.

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.

Covered Entity. An entity to which HIPAA applies, including the University because it is a Health Plan and/or a Health Care Provider that transmits any Health Information in electronic form in connection with the performance of one of the following eleven transactions: (i) Health Care claims or equivalent encounter information; (ii) Health Care payment and remittance advice; (iii) coordination of benefits; (iv) Health Care claims status; (v) enrollment and disenrollment in a health plan; (vi) eligibility for a health plan; (vii) health plan premium payments; (viii) referral certification and authorization; (ix) first report of injury; (x) health claims attachments; and (xi) other transactions that the Secretary of DHHS may prescribe by regulation. 45 C.F.R. § 160.103.

Covered Functions. Those functions performed by the University that make it a Health Care Provider, such as providing Health Care services and billing for those services, or a Health Plan. 45 C.F.R. § 164.103.

Designated Record Set. The medical and billing records about individuals; or the enrollment, payment, claims adjudication, and case or medical management records systems; used, in whole or in part, by University Personnel to make decisions about individuals, regardless of who originally created the information and that are maintained, collected, Used, or disseminated by or for a University Health Care Component.

A Designated Record Set does not include: (a) duplicate information maintained in other systems; (b) data collected and maintained for Research; (c) data collected and maintained for peer review or risk management purposes; (d) Psychotherapy Notes; (e) information compiled in reasonable anticipation of litigation or administrative action; (f) employment records; (g) education records covered by FERPA; (h) information subject to 42 USC 263a (CLIA) or

exempt under 42 CFR 493.3(a)(2) (CLIA); and (i) source data interpreted or summarized in the individual's medical record (example: pathology slide and diagnostic films). 45 C.F.R. § 164.501.

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

Device Inventory. A list of all University-owned, University-leased, or personally-owned hardware and electronic devices used to create, store, or transmit PHI for or as part of University Business. The Device Inventory should include desktops, laptops, tablets, smart phones, flash drives, external hard drives, medical devices, and medical and any other devices that contain PHI, such as scanners, fax machines, and copiers.

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

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

Direct Treatment Relationship. A treatment relationship between an individual and a Health Care Provider that is not an Indirect Treatment Relationship. (See, Indirect Treatment Relationship.) 45 C.F.R. § 164.501.

Electronic Protected Health Information (ePHI). Individually identifiable health information maintained or transmitted in electronic form or media.

Encryption. Use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key. Used to make data unusable, unreadable, or indecipherable to unauthorized persons, for purposes of HIPAA compliance.

Genetic Information. Includes an individual's genetic tests; the genetic tests of an individual's family members; the manifestation of a disease or disorder in an individual's family members; an individual's request for or receipt of genetic services; or an individual's or an individual's family member's participation in clinic research that includes genetic services. Genetic Information also includes that concerning a fetus carried by an individual or an individual's family member and an embryo legally held by an individual or an individual's family member utilizing assisted reproductive technology. Gender and age are NOT considered Genetic Information. 45 CFR § 164.103.

Genetic Services. Include genetic tests; genetic counseling; and obtaining, interpreting, or assessing Genetic Information. 45 CFR § 164.103.

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.

Health Care Component(s). The designated parts of the University, a Hybrid Entity, that are covered by HIPAA. The Health Care Components of the University of Oklahoma include the parts of the following areas that provide Covered Functions: (a) College of Medicine – Oklahoma City, including OU Physicians; (b) OU School of Community Medicine (formerly College of Medicine – Tulsa), including OU Physicians-Tulsa; (c) College of Pharmacy; (d) College of Dentistry; (e) College of Nursing; (f) College of Allied Health; (g) College of Public Health; (h) Development Office; (i) Goddard Health Center; (j) Athletics Department Center for Athletic Medicine and Psychological Resources for OU Student-Athletes;* (k) Information Technology; (l) Internal Auditing; (m) Office of Legal Counsel; (n) HSC Financial Services; (o) NC Financial Support Services; (p) Office of Compliance; (q) Human Research Participant Protection Program/Institutional Review Board; (r) HSC Student Counseling Services;* (s) University Printing Services; and (t) Waste Management – Norman Campus.

* By policy only

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

Health Care Operations. 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 Workforce Member and patients with information about treatment alternatives; and related functions that do not include treatment;

(b) Reviewing the competence or qualifications of Health Care professionals; evaluating practitioner and provider performance and Health Plan performance; conducting training programs in which students, trainees, or practitioners in areas of Health Care learn under supervision to practice or improve their skills as Workforce Members; training of non-Health Care professionals; and 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 and 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 HIPAA 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; (4) creating de-identified Health Information or a limited data set; and (5) fundraising for the benefit of a Health Care Component(s). 45 C.F.R. § 164.501.

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.

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.

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

Health Plan. An individual or group Plan that provides, or pays the cost of, medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-1(a)(2)) and includes the following, singly or in combination: (i) A group Health Plan; (ii) Health Insurance Issuer; (iii) an HMO; (iv) Part A or Part B of the Medicare program under Title XVIII of the Act; (v) the Medicaid program under title XIX of the Act, 42 U.S.C. 1396, et seq; (vi) the Voluntary Prescription Drug Benefit Program under Part D of title XVIII of the Act, 42 U.S.C. 1395w-101 through 1395w-152; (vii) an issuer of a Medicare supplemental policy (as defined in section 1882(g)(1) of the Act, 42 U.S.C. 1395ss(g)(1)); (viii) an issuer of a long-term care policy, excluding a nursing home fixed indemnity policy; (ix) an employee welfare benefit Plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers; (x) the Health Care program for uniformed services under Title 10 of the United States Code; (xi) the veterans' Health Care program under 38 U.S.C. chapter 17; (xii) the Indian Health Service program under the Indian Health Care Improvement Act, 25 U.S.C. 1601, et seq; (xiii) the Federal Employees Health Benefits Program under 5 U.S.C. 8902, et seq; (xiv) an approved State Child Health Plan under Title XXI of the Act, providing benefits for child health assistance that meet the requirements of section 2103 of the Act, 42 U.S.C. 1397, et seq; (xv) the Medicare Advantage program under Part C of title XVIII of the Act, 42 U.S.C. 1395w-21 through 1395w-28; (xvi) a high risk pool that is a mechanism established under State law to provide health insurance coverage or comparable coverage to eligible individuals; (xvii) any other individual or group Plan, or combination of individual or group Plans, that provides or pays for the cost of medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)).

Health Plan excludes: (i) Any policy, Plan, or program to the extent that it provides, or pays for

the cost of, excepted benefits that are listed in section 2791(c)(1) of the PHS Act, 42 U.S.C. 300gg-91(c)(1); and (ii) a government-funded program (other than one listed in paragraph (1)(i)-(xvi) of this definition): (A) whose principal purpose is other than providing, or paying the cost of, Health Care; or (B) whose principal activity is: (1) the direct provision Care to persons. Implementation specification means specific requirements or instructions for implementing a standard.

HIPAA. The Health Insurance Portability and Accountability Act of 1996, as amended.

HIPAA Policies or Policies. This set of policies and related forms and procedures relating to the protection and confidentiality of Protected Health Information.

HIPAA Program Employees. Those employees who have direct responsibilities under the HIPAA policies, including the University Privacy Official, the HIPAA Security Officer, the HIPAA Compliance Auditor, Office of Compliance staff, the HIPAA Project Manager, and the individuals designated by them.

HIPAA Regulations. The regulations issued by the Department of Health and Human Services implementing the privacy and security requirements of the Health Insurance Portability Act of 1996 (HIPAA), 42 CFR Parts 160 and 164.

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

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 (the parts of the Covered Entity that are subject to HIPAA.). 45 C.F.R. § 164.504. (The University is a Hybrid Entity. See also, Health Care Components.)

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 the Health Care Provider who provides the services or products or reports to the individual. 45 C.F.R. § 164.501.

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

Information Security Incident. See Security Incident.

Information Systems. Hardware, software, and information and data applications used to access, create, store, or transmit PHI for or as part of University Business.

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

164.501.

Integrity. The property that data or information have not been altered or destroyed in an unauthorized manner.

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 empowered by law to: (i) investigate or conduct an official inquiry into a potential violation of law; or (ii) prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law. 45 C.F.R. § 164.103.

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

Malicious Software. Software that is designed to damage or disrupt an Information System, including viruses, worms, Trojan Horses, Remote Call Programs, and other malicious code.

Marketing. See HIPAA *Marketing* policy.

Minimum Necessary. See HIPAA Minimum Necessary Access Rule policy.

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 University clinic and an affiliated hospital). 45 C.F.R. § 164.103.

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. See http://www.hhs.gov/hipaa/for-professionals/special-topics/mental-health/index.html.

Password. A confidential Authentication composed of a string of characters. See IT *Password Management* policy for each campus

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

Physical Safeguards. Physical measures, policies, and procedures designed to protect the University's electronic Information Systems and related buildings and equipment from natural and environmental hazards and unauthorized Access.

Personal Representative. See HIPAA *Personal Representative* policy.

Protected Health Information or PHI. Individually Identifiable Health Information that is

transmitted by, or maintained in, electronic media or any other form or medium that relates to:

1.) The individual's past, present, or future physical or mental health or condition,

2.) The genetic information of the individual,

3.) The provision of healthcare of the individual, and/or

4.) The past, present, or future payment for the provision of health care to the individual

and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual. 45 C.F.R. §160.103.

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

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

Psychotherapy Notes **exclude medication, prescription, and monitoring; counseling session 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, treatment plan, symptoms, prognosis, and progress to date. 45 C.F.R § 164.501.**

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

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

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

Risk. The likelihood that a specific threat will exploit a certain vulnerability, as well as the resulting impact of that event.

Risk Assessment. The process of identifying, estimating, and prioritizing Security risks, in each HCC and on each campus.

Risk Management. The program and supporting processes to manage a Security risk that includes:

1.) establishing the context for risk-related activities;
2.) assessing risk
3.) responding to risk once determined; and
4.) monitoring risk over time.

Risk can be managed by Risk Mitigation, Risk Acceptance, and Risk Avoidance.

Security Measures. All of the policies, procedures, standards, and controls that are in place to protect ePHI.

Security Incident. Examples of Information Security Incidents include lost laptops or smart phones, hacking, password cracking, computer virus infection, denial of service attack, or violation of acceptable use of Information Systems, that contain PHI, such as.

(a) The attempted or successful unauthorized Access, Use, Disclosure, modification, or destruction of Protected Health Information or interference with system operations in an Information System.

(b) A security-related incident that is known to or may negatively impact the Confidentiality, Integrity, or Availability of Protected Health Information.

(c) A violation or imminent threat of violation of Information System policies, standards, or practices

Information Security Incidents do not include adverse events that are not security-related, such as natural disasters and power failures.

Substance Use Disorder Records/Part 2 Records. Any information, whether recorded or not, that is created, received, or acquired by a 42 CFR Part 2 program relating to a patient (e.g., diagnosis, treatment and referral for treatment information, billing information, emails, voice mails, and texts). These records include both paper and electronic records that are maintained in connection with the performance of a federally-assisted program or activity relating to substance use disorder education, prevention, training, treatment, rehabilitation, or research. For the purposes of Part 2, this definition does not include tobacco or caffeine use. Under Part 2, a federally-assisted substance use disorder program may release patient identifying information only with the individual's written consent, pursuant to a court order, or under a few limited exceptions. Contact the Office of Legal Counsel for assistance.

Technical Safeguards. Technology and the related policies and procedures for use of the technology that protect storage, maintenance, and transmission of ePHI including but not limited to authentication requirements, password controls, audit trails, email encryption, and internet use.

Treatment. The provision, coordination, or management of Health Care and related services. 45 C.F.R. § 164.501.

Treatment includes: (a) the coordination or management of Health Care by a Health

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

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

University Business. Work performed as part of an employee's job responsibilities, or work performed on behalf of the University by faculty, staff, volunteers, students, trainees, 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.

In the context of laptop and portable device use, University Business includes, but is not limited to, the use of a laptop or device to access University email and to access non-public University systems, networks, or data in the performance of work for the University.

University Personnel. Faculty, staff, volunteers, students and trainees, 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 (also referred to as Workforce Member). 45 C.F.R. § 160.103.

Use. With respect to Individually Identifiable Health Information, the sharing, application, utilization, examination, or analysis of such information **within** the University between and by Health Care Components. 45 C.F.R. § 164.103. (But see, Disclosure.)

User. A person or entity authorized to access ePHI.

Violation. Failure to comply with a HIPAA Regulation or a HIPAA Policy. 45 C.F.R. § 160.103. See also, Breach.

Workforce Member. See University Personnel.

Workstation. An electronic computing device, such as a desktop, laptop, or other device that performs similar functions, as well as the electronic media stored in its immediate environment. PHI may not be stored on unencrypted workstations that are capable of being encrypted.

II. REFERENCES

A. 45 CFR 160.103
B. 45 CFR 164.304; 501
C. Applicable IT Security policies
D. Applicable Human Research Participant Protection policies

UNIVERSITY OF OKLAHOMA

HIPAA Policies

Title: Privacy Official – Designation and Responsibilities	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Last Revised:** 4/1/18

I. PURPOSE

To provide for the designation of a University Privacy Official, provide contact information as required by the HIPAA Regulations, and identify the responsibilities of the University Privacy Official.

II. POLICY*

The Board of Regents of the University of Oklahoma shall designate a University Privacy Official, whose responsibilities, include, but are not limited to:

A. Ensuring that necessary and appropriate HIPAA policies and forms are developed, implemented, and maintained to safeguard the Protected Health Information (PHI) of the University, in coordination with the HIPAA Security Officer and other involved offices. This includes:

1. Reviewing, updating, and developing HIPAA policies and forms as needed to ensure reasonable and appropriate protection of PHI.

2. Retaining all versions of HIPAA policies, forms, and related documentation for at least six years from the date of creation or date of last effect, whichever is longer.

3. Informing all HCCs and their Workforce Members of the HIPAA policies, forms, and related documentation through announcements, training, and publications.

4. Answering questions regarding the content of the policies, forms, and Notice of Privacy Practices.

B. Managing the University's HIPAA Compliance program.

C. Overseeing the HIPAA Security Program and, with the Director of Compliance, supervising the HIPAA Security Officer.

D. Providing day-to-day guidance and direction to the HCCs through their identified points of contact on HIPAA-related matters.

E. Managing the investigation and resolution of reported and discovered HIPAA violations and breaches. See HIPAA *Breach of Unsecured PHI/ePHI* policy.

*Capitalized terms are defined in HIPAA *Definitions* policy

F. Providing training to HCCs and their Workforce Members on HIPAA policies, forms, and regulations. Training materials should include a test or other opportunity to demonstrate understanding of the information presented.

G. Auditing compliance of the HCCs with the HIPAA Privacy-related policies, in cooperation with Internal Audit, and the HIPAA Program Employees as described in the HIPAA Compliance Audit Program Policy.

H. Advising the General Counsel, Director of the Office of Compliance, and University administration, as appropriate, of HIPAA risks and concerns.

III. PROCEDURE

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

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

IV. REFERENCES

A. HIPAA Privacy Regulations, 45 CFR 164.530

UNIVERSITY OF OKLAHOMA

HIPAA Policies

Title: Security Officer – Designation and Responsibilities	**Approved:** January 1, 2014
Effective Date: January 1, 2014	**Revised:** 11/15/16; 4/1/18

I. PURPOSE

To identify the responsibilities of the University's HIPAA Security Officer.

II. POLICY*

The Board of Regents of the University of Oklahoma shall approve the appointment of the HIPAA Security Officer, whose responsibilities include, but are not limited to:

A. Ensuring that necessary and appropriate HIPAA Security policies are developed, implemented, and maintained to safeguard the Integrity, Confidentiality, and Availability of electronic PHI (ePHI) of the University, in coordination with the University Privacy Official and other involved offices by:

1. Reviewing, updating, and developing HIPAA Security policies in conjunction with the University Privacy Official as needed to ensure reasonable and appropriate protection of ePHI.

2. Retaining all versions of HIPAA Security policies and related documentation for at least six years from the date of creation or date of last effect, whichever is longer.

3. Informing all HCCs and their Workforce Members of the HIPAA Security policies and related documentation through announcements, training, and publications.

B. Providing training to HCCs and their Workforce Members on HIPAA Security policies, forms, and regulations. Training materials should include a test or other opportunity to demonstrate understanding of the information presented.

C. Auditing compliance of the HCCs with the HIPAA Security-related policies, in cooperation with Internal Audit, the Office of Compliance, and the University Privacy Official, as described in the HIPAA Compliance Audit Program Policy.

D. Performing and/or overseeing the University's annual HIPAA Security Risk Assessments, including any that are required to be performed by HCCs, and developing and reviewing management plans for identified risks and vulnerabilities, in consultation with IT Security and HIPAA Program Employees.

E. Providing day-to-day guidance and direction to the HCCs through their identified points of contact on HIPAA Security-related matters.

F. Assisting or coordinating with the University Privacy Official in investigating and resolving reported and discovered HIPAA violations and breaches. See HIPAA *Breach of Unsecured PHI/ePHI* policy.

G. Advising the Director of the Office of Compliance, University Privacy Official, and University administration, as appropriate, of HIPAA Security risks and concerns.

III. REFERENCES

A. HIPAA Security Regulations, 45 CFR 164.308(a)(2)
B. HIPAA Security Regulations,45 CFR 164.316

UNIVERSITY OF OKLAHOMA

HIPAA Policies

Title: Access to Own Protected Health Information	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Last Revised:** 2/1/16; 4/1/18

I. PURPOSE

To address patients' (or patients' attorney/personal representative) access to their Protected Health Information maintained by the University in a Designated Record Set. (For patient request to share PHI with others, see HIPAA *Authorization to Use or Disclose PHI – Other Than to Patient* policy.)

II. POLICY*

A. Rights to Access

The University will permit patients to inspect and obtain a copy of their Protected Health Information that is included in a Designated Record Set maintained by a Health Care Component, for as long as the Protected Health Information is maintained in the Designated Record Set. If the same information is kept in more than one Designated Record Set or in more than one location, the University has to produce the information only once per request for access.

The patient must complete a HIPAA *Request for Health Information/Treatment Records* form (for use when patient wants own/child's records) or similar form or a HIPAA *Authorization to Release Health Information/ Treatment Records* form (for use when a patient wants records released to a third party), or similar form, as required in HIPAA *Authorization to Use or Disclose PHI* policy.

Unless an exception applies, patients shall be granted access to their PHI maintained in a Designated Record Set, including records received from other providers used to make Treatment decisions.

The University may charge patients requesting a copy of their own (or their minor child's) PHI a fee not to exceed actual or average costs for copies of Protected Health Information, as long as the fee is consistent with any limit set by state and federal law. Current charges are available on the HIPAA webpage and/or HIPAA Authorization forms.

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

The University must arrange with the patient for a convenient time and place to inspect or obtain a copy of the Protected Health Information or mail or fax a copy of the information at the patient's request. (See HIPAA *Administrative and Physical Safeguards* policy for information on emailing PHI.) A Health Care Component may discuss the scope, format, and other aspects of the request for access with the patient as necessary to facilitate the timely provision of access.

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

B. Psychotherapy Notes

A patient does not have the right to access Psychotherapy Notes relating to him/herself except (i) to the extent the patient's treating professional approves the access in writing; or (ii) if the patient obtains a court order authorizing such access. (See HIPAA *Mental Health Records, Substance Abuse and Psychotherapy Notes* and *Definitions* policies.) Requests for Psychotherapy Notes cannot be combined with request for other PHI; a separate Request or Authorization form must be submitted.

C. Denial of Right to Access

A patient may be denied access to Protected Health Information under the limited circumstances listed below. **The following exceptions should be narrowly construed and rarely used.** The University must, to the extent possible, give the patient access to any other Protected Health Information requested, after excluding the Protected Health Information to which access is being denied.

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

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

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

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

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

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

7. Personal Representative. The University may deny access to Protected Health Information if the request is made by a patient's Personal Representative and a licensed Health Care Professional has determined, in the exercise of professional judgment, that access by the Personal Representative is reasonably likely to cause substantial harm to the patient or another person. (See HIPAA *Personal Representative* policy.) (See Paragraph II. D. below.)

8. Psychotherapy Notes. See Paragraph II. B above.

9. CLIA Information. The University may deny access to PHI that is subject to 42 USC 263a if such access would be prohibited by law or to PHI that is exempt under 42 CFR 493.3(a)(2), CLIA. The Office of Legal Counsel or the University Privacy Official should be contacted prior to denying access on this basis.

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

D. Review of Denied Access

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

III. PROCEDURES

A. Rights to Access

1. All patients must make their requests for access to their PHI in writing using the University's Request for Health Information/Treatment Records (Request form) or Authorization to Release Health Information/Treatment Records (Authorization form) or another form that complies with HIPAA and Oklahoma law. Patients making their request for access to PHI (excluding immunization records) by telephone or e-mail must be sent a copy of the

Authorization form or referred to the University's HIPAA forms webpage for patients. **Verification of the requester's identity must be obtained prior to granting access to the Protected Health Information.** (See HIPAA *Verification of Identity* policy.) The form must be maintained in the patient's medical record for a minimum of six (6) years. For immunization record requests, See HIPAA *Required and Permitted Uses and Disclosures* policy, paragraph II.B.8.

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

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

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

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

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

B. Denial of Right to Access

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

C. Review of Denied Access

Health Care Components are required to promptly forward requests for review of denial to a Reviewer approved by the University Privacy Official. The Reviewer is required to review the denial within a reasonable period of time, but no later than thirty (30) calendar days after receiving the request for review. Access to Protected Health Information must be provided to the

patient in accordance with the determination of the Reviewer. The Health Care Component shall notify the patient making the request promptly, in writing, of the Reviewer's decision, a copy of which must be filed in the patient's medical record and sent to the University Privacy Official upon request.

IV. REFERENCES

A. HIPAA Privacy Regulations, 45 CFR 164.524

UNIVERSITY OF OKLAHOMA

HIPAA Policies

Title: Accounting of Disclosures	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Last Revised:** 2/1/16; 4/1/18

I. PURPOSE

To provide for a log of certain Disclosures of Protected Health Information.

II. POLICY*

Patients have the right to know who the University has disclosed their PHI to, so each Health Care Component must record certain Disclosures on an Accounting of Disclosure log. Patients may request a copy of this log. The log 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) of the PHI it maintains in a Designated Record Set. Business Associates also must maintain a log of Disclosures they make of the PHI maintained in a Designated Record Set.

A. Accounting Requirements – General

Each Health Care Component shall maintain an Accounting of Disclosure log for each patient. A sample log is available on the HIPAA website. The log must include all Disclosures of PHI maintained in a Designated Record Set, **except** for Disclosures:

1. to carry out Treatment, Payment, or Health Care Operations;
2. to patients of Protected Health Information about them;
3. incident to a Use or Disclosure otherwise permitted or required by the HIPAA Regulations (such as to Business Associates or Personal Representatives);
4. pursuant to the patient's HIPAA *Request for Health Information/Treatment Records* form or a HIPAA *Authorization to Release Health Information/ Treatment Records* form (See HIPAA *Access to Own Protected Health Information* policy);
5. to persons involved in the patient's care; or to notify or assist in the notification of a family member, Personal Representative, or other person responsible for the care of the patient of the patient's location, general condition, or death;
6. for national security or intelligence purposes;
7. to Correctional Institutions or Law Enforcement officials to provide them with information about a person in their custody;
8. as part of a limited data set (See HIPAA *Limited Data Sets* policy); or
9. that occurred prior to April 15, 2003.

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

*Capitalized terms are defined in HIPAA *Definition* policy

B. Accounting Requirement – Research Involving More than 50 Participants

If a Health Care Component makes Disclosures of Protected Health Information for an approved Research purpose for 50 or more individuals, the log (sample available on the HIPAA webpage) may include only the following:

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 a log of Research Disclosures and if it is reasonably likely that the Protected Health Information of the patient requesting the log was Disclosed for Research, the Health Care Component shall assist the patient in contacting the entity that sponsored the Research and the researcher, if requested.

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

C. Suspension of Right to Log

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

III. PROCEDURE

A. A patient must request a log of Disclosures in writing using the HIPAA *Request for Accounting of Disclosures* form. **Verification of the requester's identity must be obtained prior to granting the request.** (See HIPAA *Verification of Identity* policy.) Health Care Components receiving a request for an accounting log by telephone or e-mail shall send a copy of the Request form or refer the patient to the HIPAA forms webpage. The Request form must be maintained in the patient's medical record for a minimum of six (6) years.

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

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

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

1. the date of the Disclosure;

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

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

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

For Research-related Disclosures, see Section II.B. above.

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

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

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

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

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

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

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

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

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

IV. REFERENCES

A. HIPAA Privacy Regulations, 45 CFR 164.528

UNIVERSITY OF OKLAHOMA

HIPAA Policies

Title: Authorization to Use or Disclose PHI – Other Than to Patient	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Last Revised:** 2/1/2016; 4/1/2018

I. PURPOSE

To establish Authorization form and procedure requirements for Uses and Disclosures of Protected Health Information to third parties other than for Treatment, Payment, and Health Care Operations. If a patient wants to a copy of her own records, for herself or her attorney/personal representative, see HIPAA *Patient Access to PHI* policy.

II. POLICY*

Health Care Components cannot Use or Disclose Protected Health Information for purposes **other** than Treatment, Payment, and Health Care Operations without a valid written Authorization from the patient, except as otherwise permitted by these Policies or law. The Use or Disclosure made must be consistent with the patient's written Authorization (See III.B. below). The University's Authorization form is available on the HIPAA website.

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

A. Medical/Billing Records

University Personnel must obtain a HIPAA *Authorization to Release Health Information/Treatment Records* form from the patient (or the patient's Personal Representative) for any Use or Disclosure of PHI, including but not limited to requests from the patient to share her PHI with third parties. If a patient wants to a copy of her own records, for herself or her attorney or personal representative, see HIPAA *Patient Access to PHI* policy.

B. Psychotherapy Notes

University Personnel must obtain an Authorization for any Use or Disclosure of Psychotherapy Notes, except in limited circumstances. See, HIPAA *Mental Health Records and Psychotherapy Notes* policy. The Authorization must be separate from an Authorization to release other health records or information.

C. Fundraising

Health Care Components must obtain an Authorization to Use and Disclose PHI for certain fundraising activities. See HIPAA *Fundraising* policy.

D. Sale of PHI

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

E. Marketing

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

F. Substance Use Disorder Records

Information authorized for release pursuant to an Authorization might specify Substance Use Disorder Records protected under federal and/or state law. Re-disclosure of such records by the recipient is prohibited without specific Authorization, as stated on the Authorization form. Release of Substance Use Disorder Records in any format requires use of the substance use disorder cover sheet language.

G. Conditioning of Authorizations

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

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

H. Revocation of Authorizations

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

III. PROCEDURES

There are two University forms used for the release of PHI. If an individual wants a copy of her records released to herself or her attorney/Personal Representative, the individual must complete a HIPAA *Request for Health Information/Treatment Records* form. A similar form, such as a HIPAA-compliant Authorization form, may also be accepted.

If an individual wants her records released to a third party, the individual must complete a

HIPAA-compliant Authorization form, such as the University's HIPAA *Authorization to Release Health Information/Treatment Records* form. The Oklahoma State Board of Health's Oklahoma Standard Authorization Form may also be accepted, in compliance with Oklahoma law.

A. The Authorization or Request form must be in plain language and the Authorization must contain all of the core elements required by the Privacy Regulations and State law, including the patient's or the patient's Personal Representative's signature.

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

1. the expiration date has passed or the expiration event is known to have occurred;
2. the Authorization has not been filled out completely;
3. University Personnel have knowledge that the Authorization has been revoked;
4. University Personnel have knowledge that some material information in the Authorization is false;
5. the Authorization was obtained by improperly conditioning Treatment upon its receipt;
6. the Authorization is missing one of the elements required by the Privacy Regulations or State law (list available from the University Privacy Official);
7. the Authorization is for Psychotherapy Notes and other types of medical records (combining forms for both is prohibited);
8. the Authorization is combined with another document, resulting in a compound Authorization that is for purposes other than Research.

C. **Request for Health Information/Treatment Records form** – Prior to Using or Disclosing PHI pursuant to a HIPAA *Request for Health Information/Treatment Records* form, University Personnel must ensure the form is complete and signed by the patient or the patient's attorney/Personal Representative. Health Care Components may contact the Office of Legal Counsel or the University Privacy Official for help in determining whether a Request is valid.

D. 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, if the patient wants one.

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

IV. REFERENCES

A. HIPAA Privacy Regulations, 45 CFR 164.508

UNIVERSITY OF OKLAHOMA

HIPAA Policies

Title: Breach of Unsecured PHI/ePHI	**Approved:** September 23, 2009
Effective Date: September 23, 2009	**Last Revised:** 2/1/2016; 4/1/2018

I. PURPOSE

A. To provide for notification in the case of Breaches of unsecured Protected Health Information. For purposes of these requirements, "unsecured" Protected Health Information or PHI means Protected Health Information that is not secured through the use of approved technologies or methodologies that make Protected Health Information unusable, unreadable, or indecipherable to unauthorized individuals, as determined by HIPAA Program Employees. A Breach is the acquisition, Access, Use, or Disclosure of Protected Health Information in a manner not permitted under HIPAA that compromises the security or privacy of the Protected Health Information.

B. To establish the requirements regarding the protection of PHI, including ePHI, that each Health Care Component must comply with and the notification that must occur in the event of a Breach of unsecured PHI.

II. POLICY*

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

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

III. PROCEDURE

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

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

1. **Encryption** – Each Health Care Component will comply with the encryption technologies and methodologies implemented by its Information Security group to enhance the protection of ePHI. Refer to relevant IT policies (available on the Information Technology webpage for each campus) for encryption

requirements.

2. **Destruction** – Each Health Care Component will comply with the destruction techniques implemented by its IT Security group and the University HIPAA policies that render PHI unusable, unreadable, or indecipherable in any format.

   a. Destruction techniques used for ePHI must render the ePHI unusable, unreadable, and indecipherable. Contact Information Technology for assistance.

   b. Destruction techniques for paper PHI must render the PHI unusable, unreadable, and indecipherable. Refer to HIPAA *Administrative and Physical Safeguards* policy for destruction requirements of paper records containing Protected Health Information.

For additional information on the guidelines and standards of encryption and destruction methods of electronic PHI, Health Care Components should contact their Information Technology representative.

B. Notification of Breach

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

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

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

   b. Substitute notice in the case in which there is insufficient or out-of-date contact information (excluding for next-of-kin or personal representative),. In cases of fewer than 10 individuals for whom there is insufficient or out-of-date contact information, substitute notice may be by an alternative form of written notice, telephone, or other means.

   c. In the case of 10 or more individuals for whom there is insufficient contact information, conspicuous posting for 90 days consecutive days on the

University's home page (and of the Health Care Component, if it maintains one) and/or notice in major print or broadcast media, each including a toll-free number that is active for at least 90 days, will occur, as determined by the University Privacy Official.

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

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

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

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

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

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

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

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

4. **Notice Involving Business Associates** - If a Breach is caused or discovered by a Business Associate of the University, the University Privacy Official shall work with the Business Associate to address the notice requirements, in accordance with the terms of the Business Associate Agreement in place between the parties, as well as with HIPAA. The timing and content of any required notice shall be in accordance with the Agreement and applicable law.

5. **Law Enforcement Requirement to Delay Notice** - If a Law Enforcement Official informs the University or its Business Associate that a required notice would impede a criminal investigation or threaten national security, the University Privacy Official shall (a) comply with Law Enforcement's written request for a delay for the time

period specified in the statement or (b) document Law Enforcement's verbal request, specifying the time for which the delay is required and the identity of the Law Enforcement Official making the request and delay the notice for up to 30 days, unless a written statement with a longer delay period is provided.

C. Tracking

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

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

IV. REFERENCES

A. HIPAA Privacy Rules, 45 CFR 164.400, et seq.
B. NIST SP 800-111, *"Guide to Storage Encryption Technologies for End User Devices"* and SP 800-88, *"Guidelines for Media Sanitization"* as updated or revised
C. 24 O.S. 163.5, Breach Notification Reporting Process (available from the University Privacy Official)
D. Sample Notice Letter (available from the University Privacy Official)
E. Information Technology Security policies, http://it.ouhsc.edu/policies
F. HIPAA HITECH Act Regulations, 42 CFR: Parts 412, 413, 422 and 495

UNIVERSITY OF OKLAHOMA

HIPAA Policies

Title: Communication by Alternative Means	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Revised:** 2/1/2016; 4/1/2018

I. PURPOSE

To permit patients to request to receive communication of Protected Health Information by means or at locations other than those typically used by the University or a Health Care Component.

II. POLICY*

The University will permit patients to request, and will accommodate reasonable requests by patients, to receive communications of Protected Health Information by means or at locations other than those typically used by the University or a Health Care Component.

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

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 acceptance of an alternative means of communication on receiving: (a) information as to how payment will be handled, if applicable and (b) an alternative address or other method of contact.

III. PROCEDURE

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

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

If the patient does not request an alternative means of communication from any other Health

Care Components, the Health Care Component that received the initial request shall process the request in accordance with its internal procedures and send a copy of the request form and the denial form, if applicable, to the University Privacy Official upon request.

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

Questions regarding the reasonableness of a particular request should be discussed with the University Privacy Official.

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

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

F. The Health Care Component manager or designee must inform the billing department and other departments, providers, and Business Associates who may be communicating with the patient on behalf of the Health Care Component of the agreed–upon alternative means of communication. Health Care Components must send or make available to those departments and entities a copy of the approved Request form.

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

IV. REFERENCES

A. HIPAA Privacy Regulations, 45 CFR 164.522 (b)

UNIVERSITY OF OKLAHOMA

HIPAA Policies

Title: Complaint and Incident Reporting and Tracking	**Approved:** July 30, 2008
Effective Date: August 1, 2008	**Last Revised:** 2/1/16;4/1/18

I. PURPOSE

To establish the procedures for receiving, documenting, and tracking both (a) complaints filed by individuals about compliance with HIPAA policies and procedures, and (b) internal and external incidents regarding alleged failures to comply with the University's HIPAA policies and procedures by the University's Health Care Components and/or University Personnel. Together these are referred to as "complaints."

II. POLICY*

All complaints received regarding HIPAA compliance and incidents discovered or reported regarding HIPAA compliance, regardless of the form in which they are reported or how they are brought to a Workforce Member's attention, must be documented, reviewed, and acted upon, if necessary, by the University's Privacy Official, a HIPAA Program Employee, or their designee. Health Care Components may ask but may not require that complaints be reported on the University's HIPPA Complaint form (available on the HIPAA website.).

Documentation regarding complaints received and incidents reported and the resolution will be retained by the University Privacy Official, in written or electronic format, for at least six (6) years.

A complaint or report may be made by Workforce Members, patients, another Covered Entity, or a member of the public.

III. PROCEDURE

A. **Health Care Component Documentation** - Each Health Care Component shall designate and document an individual responsible for receiving and managing HIPAA complaints and incidents (together "complaints") involving the Health Care Component.

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

Each Health Care Component manager shall track HIPAA complaints using a process

that involves the notification of the University's Privacy Official or HIPAA Program Employee of each complaint so that the University Privacy Official can also record and track the investigation and response to each report and can coordinate in the investigation and resolution.

B. **Investigation** - The University Privacy Official or designee will be responsible for the investigation of each report, in coordination with or through the appropriate Health Care Component and, if necessary, with other affiliated entities. The individual in the Health Care Component designated to receive HIPAA complaints shall manage the investigation at the request of the University Privacy Official or designee.

C. **Investigation Record** - The Health Care Component and the University Privacy Official shall each maintain a record of each HIPAA complaint, the investigation, and the resolution (including corrective action and sanction, if any). The Health Care Component shall provide a copy of this record to the University Privacy Official upon request and at least annually.

IV. REFERENCES

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

UNIVERSITY OF OKLAHOMA

HIPAA Policies

Subject: Contingency Plans for ePHI	**Approved:** January 2, 2014
Effective Date: January 2, 2014	**Last Revised:** 11/15/16; 4/1/18

I. PURPOSE

To ensure that each Health Care Component is prepared for emergencies or disasters by ensuring that ePHI is protected and available and the Health Care Component is able to continue providing services, as appropriate.

II. POLICY*

Each Health Care Component, in consultation with its Information Technology representative, Enterprise Risk Management representative, and the HIPAA Security Officer, and in accordance with the Information Technology resource and data recovery policies and campus disaster recovery plan, shall establish and implement a contingency plan or adopt the campus contingency plan for responding to an emergency or other event that damages the Health Care Component's systems that contain ePHI.

III. PROCEDURE

Each Health Care Component that maintains ePHI shall establish, document, and implement its own or adopt the campus contingency plan that covers its Information Systems that contain ePHI. The plan must include, at a minimum, the following:

A. A Data Back-up Plan that will make it possible to retrieve exact copies of the HCC's ePHI.
    1. If the HCC maintains all ePHI on the University's secure servers, it may document that it relies on its campus Information Technology data back-up plan to comply with this requirement.
    2. If the HCC maintains ePHI on its own servers, it may model its plan on its campus Information Technology plan or develop its own. The plan must be in writing and approved by the HCC's dean or director.

B. A Disaster Recovery Plan and services that will make it possible to restore the HCC's lost ePHI.

    (**NOTE:** If the HCC maintains all ePHI on servers within designated IT campus data centers and has documentation in place with IT for Disaster Recovery Services, the HCC may rely on the University's Information Technology Disaster Recovery services. The services must be defined in the HCC's Disaster Recovery Plan.)

    Disaster Recovery Plans, at a minimum, should include the following:

    1. The conditions for activating the Disaster Recovery Plan
    2. Business, infrastructure, and resource requirements for the Plan
    3. Identification and definition of Workforce Member roles and responsibilities in the

Plan, as well as their contact information

4. Identification of on external entities to be used for restoration and requirements for and/or agreements with those entities
5. Procedures that identify recovery locations and describe the actions to be taken to resume normal operations within required timeframes
6. The order in which Information Systems or data must be recovered
7. Allowable or acceptable outage times
8. Notification and reporting procedures
9. Procedures for allowing appropriate physical access to the Facilities and Information Systems
10. Procedures for obtaining ePHI when normal access is unavailable for business continuity

C. An Emergency Mode Operation Plan that will enable the HCC to perform its critical business functions while still protecting its ePHI.

D. Testing and Revision Procedures to ensure the HCC's contingency plan is functioning and appropriate. These procedures should include, at a minimum:

1. What applications will be tested
2. The training necessary for those with assigned responsibilities
3. The types of tests involved (e.g., exercise, walk-through, real operational scenario)

If the Health Care Component relies on Information Technology for its data back-up or disaster recovery plans, it may document in its Plan that it relies on Information Technology's testing and revision procedures.

E. An Applications and Data Criticality Analysis that assesses how critical each HCC ePHI application is and whether it is sufficiently addressed in the contingency plan.

1. Each HCC manager may coordinate the data classification process with Information Security.

F. Emergency Access Procedures to allow authorized individuals to access Facilities that store ePHI and Information Systems to support the recovery and response efforts of the contingency plan.

1. HCC administration should maintain a list of emergency contacts that may assist in these efforts, such as Campus Police, Site Support, Physical Plant, and Information Technology. A copy of the list should be maintained outside of the Health Care Component.
2. HCC administration should provide its assigned Information Technology Representative/Tier 1 with the HCC's emergency after-hours contact information for the HCC's emergency contact and should have a copy of the Information Technology Representative/ Tier 1 after-hours contact information.

The Health Care Component manager or administrator shall submit the contingency plan to Information Security and the HIPAA Security Officer upon request. Either may require that additional procedures be implemented to ensure the plan complies with HIPAA Regulations and University IT and HIPAA policy.

A copy may also be provided to Enterprise Risk Management for review and recording.

IV. REFERENCES

1. 45 CFR 164.308(a)(7)
2. 45 CFR 164.310(a)(2)(i)
3. Applicable Information Technology Policies

UNIVERSITY OF OKLAHOMA

HIPAA Policies

Title: De-Identification /Re-Identification of PHI	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Last Revised:** 2/1/2016;4/1/2018

I. PURPOSE

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

II. POLICY*

De-Identified Information/Re-Identification

Health Care Components can Use and Disclose de-identified Protected Health Information, defined below, without complying with the University's HIPAA policies or the HIPAA Regulations as long as the code or other means of re-identification is not disclosed with the de-identified PHI.

Health Care Components may Use Protected Health Information to de-identify it or may Disclose Protected Health Information to a contracted Business Associate to de-identify it for the Health Care Component.

If de-identified information is re-identified, its Use and Disclosure become subject to the HIPAA policies and regulations.

Health Information that does not identify an individual and that there is no reason to believe can be used to identify the individual is "de-identified information" and is not individually identifiable, so it is not considered Protected Health Information. It is not subject to the requirements of the HIPAA Policies or Regulations.

III. PROCEDURE

A. De-Identification

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

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

1. Removal of Identifiers. The following identifiers of the patient **or of the relatives, employers, or household members of the patient** are removed and the University

has no actual knowledge that the information could be used alone or with other information to identify the individual:

a. Names

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

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

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

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

d. Telephone numbers

e. Fax numbers

f. E-mail addresses

g. Social Security Numbers

h. Medical record numbers

i. Health plan beneficiary numbers

j. Account numbers

k. Certificate/license numbers

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

m. Device identifiers and serial numbers

n. Web Universal Resource Locators (URLs)

o. Internet Protocol (IP) address numbers

p. Biometric identifiers, including fingerprints and voiceprints

q. Full face photographic images and other comparable images

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

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

B. **Re-Identification**

A Health Care Component may assign a code or other means of record identification to allow de-identified information to be re-identified (and therefore subject to HIPAA), 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 to identify the individual; and

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

IV. REFERENCES

A. HIPAA Privacy Regulations, 45 CFR 164.502(d)
B. HIPAA Privacy Regulations, 45 CFR 164.514 (a) – (c)

UNIVERSITY OF OKLAHOMA

HIPAA Policies

Subject: Development and Amendment of HIPAA Policies, Procedures, and Forms	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Last Revised:** 2/1/2016; 4/1/2018; 12/18/2018

I. PURPOSE

To outline the requirements for the development and amendment to the University's HIPAA Policies and procedures, including related forms to ensure the policies continue to meet the requirements of HIPAA, as well as the process for requesting exceptions to such.

II. POLICY*

A. The University, through its University Privacy Official and HIPAA Security Officer, will implement policies and procedures that are designed to ensure the University and its Workforce Members comply with the HIPAA regulations. It shall amend its HIPAA Policies, procedures, and related forms as necessary and appropriate to comply with changes in the law; to accommodate changes in the structure or operations of the University or its Health Care Components; and when otherwise necessary and appropriate. It will consider requests for exceptions to such through its University Privacy Official or HIPAA Security Officer.

B. The HIPAA Security Officer and the University Privacy Official shall periodically review the University's HIPAA Policies, procedures, and forms; revise them as appropriate; and notify Health Care Components of substantive changes. They must also conduct reviews of each of the following operational or environmental changes within the University that could affect the security of PHI. At a minimum, reviews of applicable policies should occur:

1. When the University is changing or adding locations or systems that maintain ePHI;

2. When a HIPAA Security Incident has occurred within or been caused by the University or a Workforce Member; and

3. When HIPAA Security regulations or IT Security policy updates are issued.

C. Each Health Care Component shall periodically review its internal HIPAA policies, forms, and procedures to ensure they continue to comply with the University's HIPAA policies, forms, and procedures. Reviews shall also be conducted:

1. When the HCC changes or adds locations or systems that maintain ePHI;

2. When a HIPAA Security Incident has occurred within or been caused by the HCC;

3. When HIPAA Security regulation, HIPAA policy, or IT Security policy updates are

issued; and

4. Upon request of the HIPAA Security Officer or IT Security Officer, University Privacy Official, or University administration.

D. The University has reserved in its Notice of Privacy Practices the right to change its HIPAA practices and amend its HIPAA 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 and after the effective date of the amendment. If any changes affect the content of the Notice of Privacy Practices itself, the University, through the University Privacy Official, shall promptly amend its Notice of Privacy Practices.

III. PROCEDURE

A. Changes or Additions to HIPAA Policies and Procedures Addressed in the Notice of Privacy Practices. In order to effectuate changes to policies and procedures addressed in the Notice of Privacy Practices, the University through the University Privacy Official and HIPAA Security Officer will:

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

2. Document the revised or new policy, in written or electronic format, and retain documentation of revisions for at least six (6) years.

3. Revise the University's Notice of Privacy Practices as required by the HIPAA Regulations to state the changed practice and make the revised Notice available as required. (See HIPAA *Notice of Privacy Practices* policy.)

B. Changes or Additions to Policies Not Addressed in the Notice of Privacy Practices. The University may adopt or amend, at any time, a policy that does not materially affect the content of its Notice of Privacy Practices. In order to implement such an amendment or adoption, the University, through the University Privacy Official or HIPAA Security Officer, will:

1. Ensure that the policy, as amended or adopted, complies with HIPAA; and
2. Document the revised or new policy, in written or electronic format, and retain documentation of the revision for at least six (6) years; and
3. Disseminate the revised or new policy to appropriate areas of the University.

C. HCC Responsibility. Upon receipt of notice of changes to the University's HIPAA policies, procedures, or forms, the HCC manager or designee shall:

1. Notify affected Workforce Members of the change and retain a copy of the notification; and
2. Update the HCC policies, procedures, or forms to incorporate the changes and make them available to its Workforce Members.

D. Exceptions. HCCs that believe an exception is required (versus convenient) must make a written request to the University Privacy Official or HIPAA Security Officer detailing the

requested exception and the basis for the exception. The University Privacy Official or HIPAA Security Officer, in consultation with University administration, as appropriate, will make the final determination following a complete review of the request, other applicable University policy, and applicable state and federal law, as well as the risks and benefits to the University.

IV. REFERENCES

A. HIPAA Privacy Regulations, 45 CFR 164.530(i)
B. HIPAA Security Regulations, 45 CFR 164.308 (a)(8)

UNIVERSITY OF OKLAHOMA

HIPAA Policies

Title: Disclosure of Immunization Records	**Approved:** March 1, 2018
Effective Date: March 1, 2018	**Last Revised:**

I. PURPOSE

To outline general required and permitted Uses and Disclosures of Immunization Records.

II. POLICY*

The University and University Personnel may Use or Disclose Immunization Records to a school without a written authorization as permitted by these HIPAA Policies and the HIPAA Regulations, summarized below.

A. Permitted Uses and Disclosures of Immunization Records

The University and University Personnel are permitted to Use or Disclose Protected Health Information of certain immunization records to a school -- without the standard Authorization form -- about an individual who is a student or prospective student of the school (or to the individual, if the requested information is for presentation to a school) if:

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

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

c. the University Personnel releasing the records receives and documents the request for the disclosure from either:

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

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

B. Verbal Requests

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

C. Other Uses and Disclosures

For other Uses and Disclosures of immunization records, University Personnel should contact the University Privacy Official or the Office of Legal Counsel.

III. REFERENCES

A. HIPAA Regulations, 45 CFR § 164.512

UNIVERSITY OF OKLAHOMA

HIPAA Policies

Title: Disclosure to Business Associates	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Last Revised:** 10/15/2016; 4/1/18

I. PURPOSE

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

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

II. POLICY*

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

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

III. PROCEDURE

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

B. HCCs must maintain a list of their Business Associates and provide it to HIPAA Program Employees upon request.

C. The University Privacy Official, in cooperation with the Office of Legal Counsel, is responsible for drafting, implementing, and updating the appropriate Business Associate language and/or agreements to comply with the requirements of HIPAA. Templates are available from the Office of Legal Counsel or University Privacy Official. All service contracts and Business Associate Agreements must be reviewed by the Office of Legal Counsel in accordance with Board of Regents of the University of Oklahoma policies.

Business Associate Agreements must include the provisions required under HIPAA and should include a provision requiring the Business Associate to cooperate with the University's current compliance audit program, as described in *HIPAA Compliance Audit Program* policy.

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

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

IV. REFERENCES

A. HIPAA Privacy Regulations, 45 CFR 164.502(e); 504(e); 164.532
B. HIPAA Security Regulations, 45 CFR 164.530; 312 (a); 314
C. Applicable Board of Regents of the University of Oklahoma policies

UNIVERSITY OF OKLAHOMA

HIPAA Policies

Title: Disclosures Required by Law	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Last Revised:** 2/1/2016; 4/1/2018

I. PURPOSE

To set out requirements pertaining to Uses and Disclosures of Protected Health Information that are Required by Law, as well as the requirements for logging them.

II. POLICY*

University Personnel may Disclose Protected Health Information without the patient's consent, Authorization, or opportunity to agree or object when required to do so by applicable state and federal laws, including those listed below and described in detail in this policy.

A. Abuse or Neglect of Children
B. Adult Victims of Abuse, Exploitation, or Criminally-Injurious Conduct
C. Coroner/Medical Examiner Requests
D. Death Reports
E. Funeral Director Requests
F. Government Functions - Specialized
G. Health Oversight Activities
H. Judicial and Administrative Procedure
   1. Court Orders
   2. Subpoenas
I. Law Enforcement Requests
J. Medicaid Program
K. Organ and Tissue Donations
L. Public Health Activities
M. Threats to Health and Safety
N. Worker's Compensation

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

III. PROCEDURE

A. Abuse or Neglect of Children.

1. Reporting Child Abuse, Neglect, or the Birth of a Chemically-Dependent Child. University Personnel who have reason to believe that a child under the age of 18 is a victim of abuse or neglect or who attend the birth of a child who tests positive for alcohol or a controlled dangerous substance are required by state law to promptly notify the Oklahoma Department of Human Services. Health Care Components should document their procedures for facilitating and coordinating these required reports.

No patient Authorization is required for this Disclosure, but it must be logged in the Accounting of Disclosure Log.

"Abuse" for purposes of this section is defined by Oklahoma law as 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 is defined by Oklahoma law as (i) failure to provide adequate food, clothing, shelter, medical care, and supervision; (ii) failure to provide special care that is necessary because of the physical or mental condition of the child; or (iii) abandonment.

a. Where to Report: Reports of child abuse or neglect must be made to the telephone hotline established by DHS, as required by state law. A written record of each report and the circumstances surrounding the report must be maintained by the Workforce Member or Health Care Component making the report. The report must contain the following:

- The names and addresses of the child and of the child's parents or other person(s) 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(s) responsible.

b. DHS and Law Enforcement Requests: Upon written request, Health Care Components also must provide copies of the results of the examination or copies of the examination on which the abuse or neglect report was based and any other clinical notes, x-rays, photographs, and other previous or current records relevant to the case (i) to Law Enforcement officers *who provide a written statement* that they are conducting a criminal investigation into the case and (ii) to employees of the Department of Human Services *who provide a written statement* that they are conducting an investigation of alleged abuse or neglect in the case. The statement must be retained for six years.

Statement forms for DHS and Law Enforcement to use for this purpose are available on the University HIPAA forms page, from the University Privacy Official, and from the Office of Legal Counsel.

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

3. Notification of Parent/Personal Representative. To the extent a report to DHS or Law Enforcement is made, University Personnel must promptly notify the Personal Representative of the child who is the subject of the report, unless University Personnel, using professional judgment, believe informing the Personal Representative would place

the Personal Representative at risk of serious harm or if they believe the Personal Representative is responsible for the abuse, neglect, or other injury and that informing the Personal Representative would not be in the best interests of the child.

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

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

No patient Authorization is required for this Disclosure, but it must be logged in the Accounting of Disclosure log.

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

"Abuse" for purposes of this section is defined by Oklahoma law as 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" is defined by Oklahoma law as 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 is defined by Oklahoma law as: (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.

a. Where to Report: Health Care Components shall provide supporting PHI to Adult Protective Services, Law Enforcement officers, or authorized public officials who provide *a written statement* that they are conducting an investigation. The statement must be retained for six years. Reports of victims of Abuse, Neglect, or Exploitation must contain the name and address of the Vulnerable Adult, the name and address of the caretaker, if any, and a description of the current location and current condition of the Vulnerable Adult and of the situation that may constitute Abuse, Neglect, or Exploitation of the Vulnerable Adult, in accordance with state law.

Statement forms for DHS and Law Enforcement to use for this purpose are available on the University HIPAA forms page, from the University Privacy Official, and from the Office of Legal Counsel.

2. Reporting Criminally-Injurious Conduct. Any University Personnel examining, attending, or treating a Vulnerable Adult patient for what appears to be criminally-injurious conduct, including, but not limited to, a misdemeanor or felony that results in bodily injury, threat of bodily injury, or death, is required by law to promptly report the matter to the local police department. The report may require the disclosure of Protected Health Information relevant to the investigation. Health Care Components should document their procedures for facilitating and coordinating these reports.

3. Notification of Patient or Personal Representative. To the extent a report to Adult Protective Services or Law Enforcement is made, University Personnel must promptly notify the patient or the Personal Representative of the Vulnerable Adult who is the subject of the report, unless University Personnel, using professional judgment, believe informing the patient or the Personal Representative would place the patient at risk of serious harm of if they believe that the Personal Representative is responsible for the abuse, neglect, or other injury, and that informing the Personal Representative would not be in the best interests of the Vulnerable Adult.

C. Coroners and Medical Examiners. University Personnel may Disclose Protected Health Information to coroners and medical examiners if necessary for them to identify a deceased person, determine a cause of death, or carry out their duties as authorized by law. To the extent necessary, such Protected Health Information may be Disclosed prior to, and in reasonable anticipation of, the patient's death. A *written request* from the coroner or medical examiner that includes the basis of the request should be obtained prior to the release and filed in the patient's medical record. The disclosure must be logged in the Accounting of Disclosure log.

D. Deaths on University Property. University policy requires that University Personnel report certain deaths of patients occurring on University property to the President of the University, or his or her designee, as well as to Law Enforcement. Types of deaths subject to investigation that should be reported include violent deaths; suspicious deaths; deaths related to disease that might constitute a threat to public health; and deaths unattended by a physician for a fatal or potentially fatal illness. Within thirty-six (36) hours of death, the Executive Dean of the College of Medicine or appropriate Health Care Component will send a written report to the Office of the Chief Medical Examiner, which must be accompanied by true and correct copies of all medical records of the University concerning the deceased patient.

The Chief Medical Examiner may require the University to produce the patient's Protected Health Information including records, documents, or other items regarding the deceased patient that are necessary to investigate the death. The requested Protected Health Information may be Disclosed without the Authorization of the patient's Personal Representative. However, the University must limit disclosure of such Protected Health Information to that specifically requested *in writing* by the Chief Medical Examiner. The request shall be retained for 6 years. The disclosure must be logged in the Accounting of Disclosure log.

E. Funeral Directors. University Personnel may Disclose Protected Health Information to funeral directors as necessary for them to carry out their duties with respect to a deceased patient. To the extent necessary, such Protected Health Information may be Disclosed prior to, and in reasonable

anticipation of, the patient's death. A *written request* from the funeral director that includes the basis of the request must be obtained prior to the release. The request shall be retained for six years. The disclosure must be logged in the Accounting of Disclosure log.

F. Government Functions - Specialized.

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

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

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

These disclosures must be logged in the Accounting of Disclosure log.

G. Health Oversight Activities. University Personnel may disclose PHI to a Health Oversight Agency for certain oversight activities authorized by law, upon receipt of a *written request* from the Agency. The request must state the purpose of the request and must be retained for six years. The Office of Legal Counsel or the University Privacy Official should be consulted prior to any release of PHI under this section. The Disclosure must be logged in the Accounting of Disclosure log.

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

1. Court Orders/Administrative Orders. A court order is a direction from the court that orders a party to produce certain specified documents. An administrative order is a direction issued from an administrative tribunal for documents. Upon the receipt of a court or administrative order for the Disclosure of medical records containing Protected Health Information, University Personnel must immediately forward the order to the University's Office of Legal Counsel or designee. The Office of Legal Counsel will advise University Personnel whether the order is valid, permitting the release, or whether additional documentation is required.

The patient whose records are being requested is not required to provide an Authorization for the Disclosure of the records requested pursuant to a court/administrative order, but the Disclosure must be logged in the Accounting of Disclosure log.

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

b. Disclosure of Substance Abuse Records. The content of these records may be Disclosed to third parties as follows: (i) in accordance with the patient's prior written Authorization; (ii) to medical personnel to the extent necessary to meet a bona fide medical emergency; (iii) to qualified personnel for the purpose of conducting scientific Research, management audits, financial audits, or program evaluation only if the patient is not identified directly or indirectly; or (iv) upon receipt of a valid court order that meets all of the requirements of 42 C.F.R. 2.13 (a) and 2.61-2.67. The Office of Legal Counsel or the University Privacy Official will determine whether the order complies with this federal regulation.

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

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

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

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

These disclosures must be logged in the Accounting of Disclosure log.

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

I. Law Enforcement Disclosures.

1. Locate or Identify an Individual. Certain limited Protected Health Information regarding a patient may be Disclosed to a Law Enforcement Official who requests it to identify or locate a suspect, fugitive, material witness, or missing person. Absent a request, the information may not be Disclosed. A request for PHI for this purpose may include a general request seeking the public's assistance in identifying a suspect, fugitive, material witness, or missing person. The individual making the request should be asked to sign the HIPAA *Law Enforcement Release* form located on the HIPAA forms page prior to providing the PHI.

a. If a request is made by a Law Enforcement Official--including OU Campus Police--for a patient's Protected Health Information, the Office of Legal Counsel shall be contacted immediately to determine whether the official is authorized to receive the PHI. If the Office of Legal Counsel determines that the request is valid, it shall notify the appropriate person(s) to provide no more than the limited information below.

b. The Disclosure of Protected Health Information to locate or identify an individual is limited to the following:

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

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

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

3. Patient Crime Victim. In addition to other Disclosures regarding potential victims of a crime, University Personnel may disclose to Law Enforcement Officials information about a patient who is or is suspected to be a victim of a crime, if (i) the patient consents to the Disclosure; or (ii) if the patient is unable to provide consent due to incapacity or emergency, if the Law Enforcement Official represents—via the Law Enforcement form or similar - all of the following: (a) that the information is needed to determine whether a violation of law by a

person other than the patient has occurred, (b) that the information is not intended to be used against the patient, (c) 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 (d) that the Disclosure is in the best interest of the patient, as determined by University Personnel using professional judgment.

Law Enforcement forms are available on the University's HIPAA forms page and from the University Privacy Official. University Personnel should consult with the Office of Legal Counsel or University Privacy Official before making any Disclosures under this provision.

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

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

Except as otherwise stated in 1-5 above, Authorization is not required for these Disclosures, which should be logged in the Accounting of Disclosures log unless Law Enforcement specifically requests they not be logged. See HIPAA *Accounting of Disclosures* policy, Section E, or contact the University Privacy Official.

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

No Authorization is required for the Disclosure. The Disclosure shall be logged in the Accounting of Disclosure log unless the Attorney General specifically requests that it not be logged. See HIPAA *Accounting of Disclosure* policy, Section E, or contact the University Privacy Official.

University Personnel may not refuse to provide the Oklahoma Health Care Authority or the Oklahoma Attorney General with access to these 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. Per Oklahoma law, the Disclosure of Protected Health Information under 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.

K. Organ and Tissue Donations. University Personnel may 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. A *written request* from the organ procurement organization that includes the basis of the request should be obtained prior to the release and must be retained for six years.

No Authorization is required for the Disclosure, which must be logged in the Accounting of Disclosure log.

L. Public Health Activities. University Personnel may Disclose Protected Health Information to (1) the appropriate public health authority authorized by law to collect or receive information for the purpose of preventing or controlling disease, injury, or disability (including birth and death); to conduct public health surveillance, public health investigations, or public health interventions; or, at the direction of a Public Health Authority, to certain foreign governments; (2) to a public health authority authorized by law to receive reports of child abuse or neglect; (3) to certain persons subject to FDA jurisdiction for limited purposes; (4) to the appropriate public health authority for notification of persons who may have been exposed to a communicable disease or may be at risk of such; and (5) to employers for certain medical surveillance work. These Disclosures should be made only after consultation with the Office of Legal Counsel or the University Privacy Official.

Disclosures to Public Health Authorities do not requirement patient Authorization. Disclosures shall be logged in the Accounting of Disclosure log unless the Public Health Authority specifically requests the Disclosure not be logged. See HIPAA *Accounting of Disclosure* policy, Section E. These permitted Disclosures shall also specifically include the following:

1. Statistical Reports. The State Department of Health is charged with tracking Health Information within the State of Oklahoma. The Department may request University Personnel to provide to the Division of Health Care Information certain Health Care information for the purpose of statistical and other similar reports. University Personnel may Disclose the requested information without the patient's written Authorization and must log the Disclosure in the Accounting of Disclosures log. This includes discharge data such as complete discharge data sets or comparable information for each patient discharged.

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

2. Birth Certificates. State law requires that 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.

No patient Authorization is necessary to disclose the information used to prepare and file the birth certificate. The Disclosure shall be logged in the Accounting of Disclosure log.

3. Death Certificates. The Authorization of the patient's Personal Representative is not required for University Personnel in charge of a patient's care to disclose information necessary

to complete the certificate of death for filing. The Disclosure shall be logged in the Accounting of Disclosure log if the death occurred on University property.

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

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

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

a. Court Order. Release of Protected Health Information may be made upon receipt of a valid court order. The order shall be retained for six years.

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

c. University Personnel Exposures. Release may be 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. The Disclosure must be logged.

d. Statistical Disclosures. Release may be made of specific medical or epidemiological information for statistical purposes in such a way that no person can be identified. See, HIPAA *De-Identified PHI/Re-Identification* policy.

e. Diagnosis and Treatment. Release may be made of Protected Health Information among University Personnel within the continuum of care for the purpose of diagnosis and Treatment of a communicable or venereal/sexually transmitted disease of the patient whose information is released. No logging is required for Disclosures made for Treatment purposes.

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

5. Newborn Hearing Tests. Every infant born in Oklahoma must be screened for the detection of congenital or acquired hearing loss. The results of the screening procedures must be reported to the State Department of Health, in accordance with state law. No Authorization is required for this Disclosure. The Disclosure must be logged on the Accounting of Disclosure log.

6. Birth Defects. The Commissioner of Health may require the University to make available the medical records of patients who have been diagnosed with birth defects or poor reproductive outcomes. The records shall be made available to the Commissioner upon written request. No patient Authorization is required for the Disclosure. The Disclosure must be logged in the Accounting of Disclosure log.

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

The Commissioner may require the University, via written request, to report the following information regarding cancerous and precancerous and tumorous diseases. No patient Authorization is required for the Disclosure. The Disclosure must be logged in the Accounting of Disclosure log.

a. The patient's name, address, age, race, sex, Social Security number, and hospital identifier or other identifier;
b. The patient's residential, family, environmental, occupational, and medical histories; and
c. The physician's name; diagnosis, stage of the disease, method of treatment; and the name and address of any facility providing treatment.

M. 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 the Use and Disclosure:

(i) is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public and the Disclosure is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat; or
(ii) is necessary for Law Enforcement Officials to identify or apprehend an individual who (a) has made a statement admitting participation in a violent

crime that University Personnel reasonably believes may have caused serious physical harm to the victim (provided that no Disclosure may be made under this circumstance if the Disclosure is made during the course of Treatment to affect the propensity to commit the criminal conduct that is the basis for the Disclosure, or actual counseling or therapy, or if the Disclosure is made during a request to initiate such Treatment); or (b) escaped from a Correctional Institution or from lawful custody.

The information that may be disclosed to avert a serious threat is limited to that listed in the Law Enforcement Disclosure section above (III.I.1). The Office of Legal Counsel or University Privacy Official should be consulted before any Disclosures of PHI are made pursuant to this provision. No patient Authorization is required for the Disclosure. The Disclosure must be logged in the Accounting of Disclosure log unless Law Enforcement specifically requests that they not be logged. See HIPAA *Accounting of Disclosure* policy, Section E.

N. Workers' Compensation. Under the Oklahoma's Workers' Compensation laws, an employer must provide an injured employee with reasonable and necessary medical care for a work-related injury. The attending physician is required to supply the employee and the employer with a full examining report of injuries found at the time of examination and proposed Treatment. At the conclusion of the Treatment, the attending physician must supply a full report of the Treatment of the injured employee to the employer. Upon written request, the provider shall also provide a copy to the Worker's Compensation Commission and/or fraud investigation unit, the carrier, and the employee or employee's dependents. The Disclosure must be logged in the Accounting of Disclosure log.

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

IV. ASSISTANCE

The Office of Legal Counsel or University Privacy Official should be contacted for assistance with any releases or Disclosures under this policy.

V. REFERENCES

A. 45 C.F.R. §164.512 (f), 514(d)(3)(iii)
B. 85A Okla. Stat. 58
C. 10A Okla. Stat. 1-2-101, 1-3-102
D. 43A O.S. 10-108
E. 63 Okla. Stat. 1-116, 1-311, 1-317, 1-503
F. 63 Okla. Stat. 1-550.2, 3, 1-551.1, 1-543

UNIVERSITY OF OKLAHOMA

HIPAA Policies

Title: Disclosures to Family and Others Involved in Patient's Care	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Last Revised:** 2/1/2016; 4/1/2018

I. PURPOSE

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

II. POLICY*

A. Individuals Involved in Care/Payment. If consistent with their Health Care Component policy, Workforce Members may Disclose Protected Health Information to a patient's family member, other relative, close personal friend, or any other person identified by the patient, as long as the Protected Health Information Disclosed is **relevant** to that person's involvement with the patient's care or Payment for the patient's Health Care and if Workforce Members determine that the Disclosure is in a the patient's best interests. If the patient is present or available, Workforce Members must first give the patient the opportunity to agree or object to the Disclosure, unless Workforce Members can infer from the circumstances that the patient does not object. Workforce Members should note this in the patient's record.

B. Notification/Location. Workforce Members may Use or Disclose Protected Health Information necessary to notify, or assist in the notification of (including identifying or locating), a family member, a Personal Representative, or another person responsible for the care of the patient of the patient's location, general condition, or death, if Workforce Members determine that the Disclosure is in a the patient's best interests. If the patient is present or available, Workforce Members must first give the patient the opportunity to agree or object to the Disclosure, unless Workforce Members can infer from the circumstances that the patient does not object. Workforce Members should note this in the patient's record.

C. Disaster Relief. Workforce Members 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, such as the Red Cross, if the Workforce Members determine that the Disclosure is in a the patient's best interests The Protected Health Information that may be released is limited to the patient's location, general condition, or death. If the patient is present or available, the Workforce Members must first give the patient the opportunity to agree or object to the Disclosure, unless Workforce Members can infer from the circumstances that the patient does not object. Workforce Members should note this in the patient's record.

D. Decedents. Workforce Members may Disclose a decedent's PHI to the decedent's family members, other relative, close personal friend, or individual previously identified by the decedent if that person was involved in the care or payment for care of the decedent prior to

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

III. PROCEDURES

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

1. Obtain the patient's agreement;

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

3. Reasonably infer from the circumstances, using professional judgment, that the patient does not object to the Disclosure and notes such in the patient's medical records.

University Personnel may elect to use the Authorization to Release Protected Health Information Verbally to Others (available on the HIPAA website) as a mechanism for documenting the patient's agreement to verbal Disclosures or may note it in the patient's medical record.

B. Patient is **Not** Present – If the patient is not present, or the opportunity to agree or object to the Use or Disclosure cannot practicably be provided because of the patient's incapacity or an emergency circumstance, Workforce Members may, using professional judgment, determine whether the Disclosure in II (A) – (D) above is in the best interests of the patient and, if so, Disclose only the Protected Health Information that is directly relevant to the person's involvement with the patient's Health Care. Workforce Members should note this in the patient's record and log the Disclosure in the Accounting of Disclosure log.

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

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

1. Whether the potential Disclosure is common practice;
2. The nature of the relationship between the parties;

3. The sensitive nature of the information being Disclosed;

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

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

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

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

IV. REFERENCES

A. HIPAA Privacy Regulations, 45 CFR 164.510(b)

UNIVERSITY OF OKLAHOMA

HIPAA Policies

Subject: Documentation Requirements	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Last Revised:** 2/1/16; 5/6/16; 4/1/18

I. PURPOSE

To establish documentation requirements as required by the HIPAA Regulations.

II. POLICY*

A. The University and each Health Care Component, as appropriate, will maintain, for at least six (6) years written or electronic copies of, the following:

1. All versions of the HCC's internal HIPAA policies and procedures;
2. All communication that is required by the HIPAA policies to be in writing, such as HCC's HIPAA forms and complaints;
3. Written or electronic copies of any HCC action, activity, or designation that is required by the HIPAA policies to be documented, such as the individuals who are responsible for actions under these policies.

At the end of the six-year period, HCCs may destroy documentation only if destruction is consistent with applicable University destruction procedures. (Additional information is available from the Office of Legal Counsel or the campus Record Retention Office.)

III. PROCEDURE

A. Documentation of HIPAA Policies and Procedures. Written or electronic copies of the University's Policies will be maintained by the University Privacy Official for at least six (6) years from the date the Policies were created or were last in effect, whichever is later. Health Care Components shall maintain copies of their department- or clinic-specific HIPAA policies and procedures, such as those related to Facility Access, Disaster Recovery, and Training, for at least six (6) years from the date the policies or procedures were created or were last in effect, whichever is later.

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

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

D. Documentation of Training Materials. Health Care Components should maintain copies of internal HIPAA-related communications, such as emails from the manager to staff regarding a HIPAA requirement or copies of training slides from staff meetings, for at least six (6) years from the date of creation. Health Care Components are also strongly encouraged to maintain copies of HIPAA articles or training materials included in their newsletters or meeting agendas for at least six (6) years.

E. Destruction of HIPAA-Related Documentation. After the six-year retention period, Health Care Components must comply with the applicable campus Record Retention policies. These policies generally require approval from the Record Retention office; Office of Legal Counsel; Enterprise Risk Management; and others. (Refer to the Campus Record Retention policy.) Health Care Components are also strongly encouraged to contact the University Privacy Official prior to destroying any HIPAA-related documentation to ensure compliance with this policy.

IV. REFERENCES

A. HIPAA Security Regulations, 45 CFR 164.316
B. HIPAA Privacy Regulations, 45 CFR 164.530 (j)
C. Campus Record Retention policies

UNIVERSITY OF OKLAHOMA

HIPAA Policies

Title: Emailing and Transmitting PHI	**Approved:** January 2, 2014
Effective Date: January 2, 2014	**Revised:** 11/15//2016; 3/22/2017; 4/1/2018

I. PURPOSE

To ensure Protected Health Information being transmitted electronically is protected from unauthorized Access.

II. POLICY*

This policy applies to all Health Care Components that transmit PHI from any electronic media device, including but not limited to desktop computers, laptop computers, tablet computers, digital copiers, scanners, and smart phones. Each HCC shall require that its Workforce Members comply with the following:

A. Electronic Transmissions - Each Health Care Component shall have in place written procedures for emailing PHI consistent with the following:

1. Minimum Necessary - Workforce Members shall observe the Minimum Necessary Rule when transmitting PHI, meaning they will send only the PHI necessary at that time.

2. Subject Line - Workforce Members shall not include PHI in the subject line of any electronic transmission. (Subject lines are not generally encrypted and are visible even on unopened messages.)

3. Email Within the University - Sending emails that contain PHI for an auhotrized purposes within the University (OUHSC.edu/OU.edu to OUHSC.edu/ou.edu) to an individual authorized to receive the PHI is acceptable. PHI should be sent as a limited data set when possible. The Minimum Necessary Rule must be observed when applicable (see HIPAA *Minimum Necessary Rule* policy).

4. Email Between OUHSC.edu and oumedicine.com E-mail Addresses - Sending emails that contain PHI for an authorized purpose between OU.EDU/OUHSC.edu and oumedicine.com email addresses is secure and therefore acceptable so long as the recipient is authorized to receive the PHI. PHI should be sent as a limited data set when possible and in accordance with the Minimum Necessary Rule, as applicable.

5. E-mail Outside the University - E-mail may be used to send PHI to an authorized recipient outside the University only for an authorized purpose to an authorized recipient. In all cases, the message must be encrypted between sender and recipient

in a manner that complies with HIPAA. See the IT Security Secure Email page (http://it.ouhsc.edu/services/infosecurity/SecureEmail.asp) for a list of entities with which OUHSC IT has established an encrypted (TLS) channel. If an encrypted channel does not exist, other options for secure transmissions include, for example, typing in the subject line **[secure]** for Health Sciences Center email accounts or **[OUENCRYPT]** for Norman Campus email accounts.

6. Email to Patients - Workforce Members must comply with the HIPAA Safeguards policy regarding emailing PHI to patients, as well as with the policy or practice of their HCC. (A HIPAA *Consent for Electronic Communication* form is available on the HIPAA website. Sample language for responding to requests from patients requesting that their PHI be sent via an unencrypted method is available below.) For OU Physicians, for example the preferred method for communicating electronically with patients is through a secure patient portal.

   a. When E-mail Encryption is Available. Subject to the Health Care Component's internal policies and procedures, University Personnel may send PHI to patients via encrypted email for permitted purposes to authorized recipients.

   b. Without Encryption Capabilities (E-Mail Communication Denial). If a patient sends an e-mail to an employee, student/trainee, or volunteer asking a health care question or requesting any type of information that would require a Disclosure of PHI, the request for response shall be declined by sending a new message (not a reply) similar to the following:

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

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

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

7. E-mail Notice - All emails initiated by a Workforce Member that contain PHI must include a confidentiality statement similar to the following, typically below the signature line:

      i. *This email, including any attachments, contains information that may be*

confidential or privileged and is intended for use by 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 email in error, please notify the sender immediately by a "reply to sender only" message and destroy all electronic and hard copies of the email and attachments.

8. Text Messaging - Workforce Members may not send PHI via unencrypted text messaging. Those who choose to use text messaging (SMS protocol) must de-identify PHI in the message or encrypt incoming and outgoing messages and ensure they use a secure gateway (e.g., HTTPS) if they send the messages over an Internet gateway. Workforce Members are cautioned, however, that if the recipient does not have the same encryption protocol, the text may not be secure. IT Security can provide additional information.

   Note: Texting physician orders is prohibited by CMS and the Joint Commission.

9. Text Pagers - Workforce Members shall exercise extreme caution when sending PHI via text pagers, as few pagers have encryption enabled. Consult IT Security.

10. Auto-Forwarding Email - Employees of Health Care components may not auto-forward email to a non-OUHSC.edu or non-OU.edu email address.

11. Digital Copiers/Scanners/Equipment - Health Care Components using digital copiers, scanners, fax machines, and medical and other equipment that transmits or stores PHI, even temporarily, must verify that appropriate data security features (e.g., encryption, overwriting) are enabled. In addition, before the equipment is returned to the vendor, transferred, surplussed, or otherwise disposed of, the Health Care Component must take steps to ensure the hard drive is destroyed or completely overwritten. These steps may include, but are not limited to, notifying the Purchasing Department to impose these requirements on the vendor during the contracting process or working with IT Security prior to retiring, disposing of, transferring, or surplussing the device to ensure the PHI is rendered unusable, unreadable, or indecipherable. (See HIPAA *Purchasing or Leasing Equipment or Contracting for Services Involving PHI* policy.)

B. Telemedicine

1. Workforce Members may use telemedicine technology if it meets AES Encryption standards for H.323 protocol communications. Contact IT Security for additional information.

2. Workforce Members shall be responsible for providing telemedicine patients with any required forms and the Notice of Privacy Practices prior to using this technology. Contact the Office of Legal Counsel for assistance.

Any questions about the security of electronic transmissions generally should be directed to IT Security or the Tier I or IT Representative supporting the HCC.

C. Electronic Documents - Documents and attachments and/or images containing PHI are expected to be stored on University network servers with appropriate security restrictions in accordance with IT Security policy, rather than on portable devices or unsecure desktop computers. (IT Security can provide specific information about these servers.) If documents and attachments and/or images cannot be stored on a University network server or are but instead are stored on a desktop computer or portable computer device, the Workforce Member must ensure that the computer or device is encrypted by contacting the appropriate Tier 1 or IT Representative supporting the computer or device.

D. Other Uses/Internet. Any other electronic transmission of PHI requires that appropriate safeguards and procedures be implemented to protect the PHI. Health Care Components and Workforce Members should contact IT Security or the HIPAA Security Officer for more information.

E. Social Media Sites. Protected Health Information shall not be posted or transmitted on social media sites, such as Facebook or Twitter. Replies to patient posts should be avoided, especially if the reply will confirm PHI. University Personnel should keep in mind that even if a patient's name is not posted, if the patient could reasonably be identified, alone or with information obtained from other sources, the information is considered Protected Health Information.

The HIPAA *Breach of Unsecured PHI/ePHI* policy and the HIPAA *Sanctions* policy shall be followed in the event a Workforce Member violates this policy, inadvertently or intentionally.

III. REFERENCES

A. 45 CFR 164.312(e)
B. HIPAA Administrative and Physical Safeguards; Minimum Necessary Rule, and Sanctions policies

UNIVERSITY OF OKLAHOMA

HIPAA Policies

Title: Facility Access Control Policy	**Approved:** January 2, 2014
Effective Date: January 2, 2014	**Revised:** 3/22/16; 11/15/16; 4/1/18

I. PURPOSE

To establish policy and procedures to limit physical Access to electronic Information Systems and to protect Facilities where PHI is stored or transmitted from unauthorized physical access, tampering, and theft.

II. POLICY*

Health Care Components must protect their PHI by controlling and monitoring physical access to their sites where PHI, including electronic information systems that contain PHI, is accessible. (Physical access to University data centers is controlled and monitored by data center staff.) Each Health Care Component must develop and implement procedures designed to control and monitor Access to areas of their Facilities where PHI is maintained.

III. PROCEDURE

A. Access Control Procedures - Each Health Care Component shall establish Facility access control procedures that must include, but are not limited to, requirements to maintain the following:

1. A current Role-Based Access Worksheet on each Workforce Member that documents permitted physical and electronic access to PHI.
2. A log of Workforce Members who have been given a key, key card, access code or similar that gives them access to Facilities or areas within the HCC where PHI is accessible. This log must be updated when Workforce Members separate from the HCC or their access needs change. The HCC manager must change any shared code, such as alarm code or cypher lock door code, when an employee who was issued the shared code leaves. If the HCC issues individual codes, the manager must delete the individual code when the individual leaves the HCC. In addition, it is recommended that the manager change shared codes at least annually, or more often if indicated by particular circumstances.
3. A log of access by the following individuals to areas where PHI is accessible. The log must include name of person, date, purpose of access, and any other relevant details, such as materials or equipment removed. The HCC manager must document by title or office who is responsible for maintaining the log.
    a. Non-Workforce Members, excluding patients and those accompanying them, who need regular or recurrent access to areas or Facilities within the HCC where PHI is maintained, such as vendors and repair workers.
    b. Physical access by individuals retrieving back-up media from the HCC, when feasible.

c. Physical access by individuals who enter the HCC's network closet or any area within the HCC that houses network or computer equipment that is used in the storage, transmission, or analysis of any ePHI at any time during its lifecycle. (See HIPAA *Tracking, Returning, and Disposing of Device and Media* policy for log description.)

4. Access control procedures, including the following:

   a. Entrances and exits to areas where PHI is accessible that are not monitored or attended must remain secured at all times. Doors must not be propped open, unless required by applicable fire code.

   b. Workforce Members with access to restricted areas must not allow unauthorized individuals -- including family members and friends -- access to those restricted areas. All Workforce Members should report to management any unidentified persons who have gained, or seek to gain, access to areas where PHI is maintained.

   c. When practicable and depending on the value and sensitivity of the equipment and PHI in the area, entrances, exits, windows, and strategic areas of the building, such as areas where the alarm consoles or network distribution areas are located, should be alarmed or monitored. If monitored, the HCC manager or designee should review recordings in a response to a report of unauthorized access and report unauthorized access to the University Privacy Official or HIPAA Security Officer.

B. Review of Physical Security - The University's Information Security Officer and HIPAA Security Officer or their designee, with the assistance of the HCC administration, shall periodically review physical security of any site storing or transmitting electronic PHI, especially after any significant change that may affect the security of data and applications at a particular HCC Facility.

C. University Data Centers — A University Data Center hosts enterprise and department servers in a managed, secure, environmentally-controlled and protected area devoted to housing computer equipment that may store, process, or transmit PHI. Health Care Components shall restrict access to any University Data Center located in their Facilities to authorized persons only and shall log such access. The campus entity charged with managing University Data Centers must comply with this policy.

D. Network Wiring/Communications Closets and Cabinets — These locations house network termination equipment including switches and routers. The HCC manager shall not share these locations with non-HCC individuals or entities and shall keep doors to any such closets or cabinets located within their Facilities locked. The manager shall limit distribution of keys and codes to prevent unauthorized access. Key and code access must be logged as required above.

IV. REFERENCES

A. 45 CFR 164.310(a)(1)
B. 45 CFR 164.310(b)
C. HIPAA Safeguards – Administrative and Physical policy
D. Applicable Information Technology Policies

UNIVERSITY OF OKLAHOMA

HIPAA Policies

Subject: Fundraising	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Last Revised:** 2/1/2016; 4/1/2018

I. PURPOSE

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

II. POLICY*

A. Health Care Components may Use (or Disclose to a Business Associate or a University-related foundation) the following Protected Health Information for the purpose of raising funds, including soliciting gifts or sponsorships without an Authorization:

(1) demographic information relating to an individual, including name, address, contact information, age, gender, and date of birth;

(2) dates of Health Care provided to an individual;

(3) department of service;

(4) treating physician information;

(5) outcome information; and

(6) health insurance status.

Any Use or Disclosure of Protected Health Information for fundraising purposes beyond (1) – (6) above requires the patient's written Authorization.

Demographic and outcome information does not include the Use or Disclosure of information about a patient's illness or Treatment.

B. A patient's demographic information, dates of receipt of Health Care services, department of service, treating physician information, outcome information, and/or health insurance status may be Used or Disclosed without the patient's Authorization for fundraising purposes only if the following requirements are met:

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

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

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

III. PROCEDURE

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

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

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

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

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

IV. REFERENCES

A. HIPAA Privacy Regulations, 45 CFR 164.514(f)
B. HIPAA Privacy Regulations, 45 CFR 164.520(b)

UNIVERSITY OF OKLAHOMA

HIPAA Policies

Subject: HCC Review of Access to ePHI Systems	**Approved:** January 2, 2014
Effective Date: January 2, 2014	**Revised:** 11/15/16; 4/1/18

I. PURPOSE

To ensure access to University-owned and University-leased electronic systems used to create, store, or transmit PHI in each Health Care Component are regularly reviewed for HIPAA compliance.

II. POLICY*

Each Health Care Component that maintains electronic systems that create, store, or transmit PHI shall have in place a review protocol for each system to ensure access to the systems is appropriate. Systems may include but are not limited to medical records systems, medical devices and equipment, and billing systems.

III. PROCEDURE

A. Review Protocol - Each Health Care Component manager or business administrator shall develop and document a review protocol that addresses, at a minimum, the following:

1. A list of the HCC's electronic systems that create, store, or transmit PHI.
2. How often reviews of each electronic system will occur.
3. How records for review will be selected (e.g., randomly, by position, by last name groupings).
4. What records will be reviewed (e.g., audit logs, access reports, security incident tracking reports).
5. How many records/employees will typically be reviewed. The number or percentage should be a representative sampling or meet other objective criteria.
6. How long and where the results will be maintained (minimum of six years).
7. Who will review the results to determine whether the activity identified was appropriate.
8. What action will be taken by the Health Care Component if unauthorized access is detected. Reference to the HIPAA *Sanctions* policy should be included.
9. A requirement that the University Privacy Official or designee be notified of any audit result that appears to indicate unauthorized access to ePHI.
10. A requirement that audits of User activity will also be performed at the request of and provided to the University Privacy Official, the University HIPAA Security Officer, and University administration.

A sample audit protocol is available from the University Privacy Official and the HIPAA

Security Officer.

B. The Health Care Component manager or business administrator shall, upon request, submit to the University HIPAA Security Officer or University Privacy Official or designee a copy of the review protocol and/or any completed reviews.

IV. REFERENCES

A. 45 CFR 164.308
B. 45 CFR 164.312(b)
C. HIPAA Sanctions policy

UNIVERSITY OF OKLAHOMA

HIPAA Policies

Title: HIPAA Compliance Audit Program	**Approved:** December 1, 2012
Effective Date: 12/1/2012	**Last Revised:** 2/1/2016; 4/1/2018

I. PURPOSE

To formalize the University's HIPAA Compliance Audit Program to ensure that the University's Health Care Components are consistently complying with the University's HIPAA policies and procedures.

II. POLICY*

The University Privacy Official, in coordination with the Office of Compliance, will maintain a HIPAA Audit Program to promote HIPAA awareness and compliance. The Program will include HIPAA Privacy and Security audits.

Documentation of all HIPAA compliance audits shall be maintained by the Office of Compliance for at least six (6) years.

III. PROCEDURE

A. The Office of Compliance shall employ (1) a HIPAA Compliance Auditor, who shall conduct and/or coordinate HIPAA Privacy compliance audits under the direction of the University Privacy Official, and (2) a HIPAA Security Officer, who shall conduct and/or coordinate HIPAA Security audits, consistent with this Policy. Audit instruments will be updated as needed by the HIPAA Program Employees to address current and ongoing HIPAA issues.

B. HIPAA Privacy Audits

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

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

   b. In-person audits of local off-site facilities where PHI is physically stored by a Health Care Component, occurring approximately every 24 months, or more often if indicated by audit results or HIPAA incidents. The off-site facilities may be audited via written compliance certification between in-person audits.

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

   d. Audits of the University's Business Associates, either in person or via written compliance certification, generally every 24 months.

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

C. HIPAA Security Audits

1. The HIPAA Security Audit Program shall operate as described in Section II.B.1.a-b, under the direction of the HIPAA Security Officer, with a copy of audit reports sent to the Director of Compliance.

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

E. Self Audits - At least twice annual self-audits will take place for each Health Care Component using a self-audit instrument developed and maintained by the HIPAA Program Employees. The HIPAA Compliance Auditor and HIPAA Security Officer shall review the self-audits and timely notify the Health Care Component or University Privacy Official if the audit indicates the need for corrective action or additional training. The Compliance Auditor or HIPAA Security Officer shall coordinate on the self-audit instrument.

F. Business Associate Audits

1. The University Privacy Official shall request a certification or documentation of ongoing HIPAA compliance from the University's off-site Business Associates approximately every 24 months.

2. The HIPAA Compliance Auditor shall perform a walk-through audit of the University's Business Associates that store PHI locally for the University.

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

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

IV. REFERENCES

A. HIPAA Security Regulations, 45 CFR §164.308, 312
B. HIPAA Privacy Regulations, 45 CFR §164.306

UNIVERSITY OF OKLAHOMA

HIPAA Policies

Title: HIPAA Security Risk Analysis and Risk Management	**Approved:** January 2, 2014
Effective Date: January 2, 2014	**Revised:** 11/15/2016; 4/1/2018

I. PURPOSE

To ensure the University's HIPAA Security risk analyses and management plans represent an accurate and thorough assessment of and response to potential risks and vulnerabilities to the Confidentiality, Integrity, and Availability of electronic PHI held by the University through its Health Care Components, as required by HIPAA.

II. POLICY*

Each Health Care Component shall, in coordination with the HIPAA Security Officer or IT Security Officer, identify potential risks and vulnerabilities to the Confidentiality, Integrity, and Availability of PHI in its area. Each HCC shall also cooperate with the University's Risk Analysis and University– or campus–wide Risk Management activities designed to prevent, detect, contain, and correct Security violations.

III. PROCEDURE

A. Health Care Component Responsibilities

1. Risk Analysis - Each Health Care Component shall conduct and/or participate in a Risk Analysis to identify potential risks and vulnerabilities to the Confidentiality, Integrity, and Availability of its PHI.

   The risk analysis shall include the following, as well as other items as may be required by Information Technology or HIPAA Program Employees:

   a. Identify controls that are in place for each Information System, such as physical security, passwords, and audit capability.

   b. Identify risks to the Information Systems and PHI, under the current controls, such as unauthorized access or loss/theft.

   c. Identify controls that are needed to address the risks, such as additional locks or system upgrades, and whether/how those controls can be implemented.

2. Risk Management - Based on the results of the Risk Analysis, the Health Care Component in coordination with the HIPAA Security Officer, IT Security Officer, and/or University Privacy Official, must develop a management plan to reduce any risks and vulnerabilities identified to a reasonable appropriate level, designed to:

   a. Ensure the Confidentiality, Integrity, and Availability of its PHI;

   b. Protect against reasonably anticipated threats or hazards to its PHI;

c. Protect against reasonably anticipated unauthorized Uses or Disclosures of its PHI; and

d. Ensure compliance with HIPAA by its Workforce Members.

3. Reporting and Resolution - The Health Care Component shall submit to the University HIPAA Security Officer a copy of the Risk Management plan it adopts to address identified risks. If the University HIPAA Security Officer, IT Security Officer, or University Privacy Official identifies additional risks or vulnerabilities or areas that need to be managed further, the Health Care Component shall cooperate to address each.

B. University/Campus Responsibilities

1. Risk Analysis – The University through it Information Technology and HIPAA Program Employees, shall conduct a University- or campus-wide Risk Analysis approximately every 48 months, or more often if indicated, such as following a major breach or major system change.

2. Risk Management - Based on the results of the Risk Analysis, the University, through its Information Technology and HIPAA Program Employees shall develop and implement a Risk Management plan to reduce any risks and vulnerabilities identified to a reasonable and appropriate level, as described in A(2)(a-d) above.

3. Reporting and Resolution - The HIPAA Program Employees shall submit to the Compliance Advisory Committee ("CAC") a copy of the Risk Management plan adopted. If the CAC identifies additional risks or vulnerabilities or areas that need to be managed further, the HIPAA Program Employees shall work to address each.

IV. REFERENCES

A. 45 CFR 164.308(a)(1)(ii)(A)&(B)
B. 45 CFR 164.306(a)(1)-(4)
C. Applicable Information Technology Policies

UNIVERSITY OF OKLAHOMA

HIPAA Policies

Title: Limited Data Sets	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Last Revised:** 2/1/2016; 4/1/2018

I. PURPOSE

To establish permitted Uses and Disclosures of limited data sets -- PHI from which specified identifiers have been removed and patient Authorization to Use or Disclosure is not required -- and the method for creating them.

II. POLICY*

A Health Care Component may Use and Disclose a limited data set only for the purposes of Research, public health, or Health Care Operations and only if the Health Care Component enters into a Data Use Agreement with the intended recipient of the limited data set. Disclosures made under a Data Use Agreement are not required to be logged on the Accounting of Disclosures log.

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

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

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

If University Personnel receive a limited data set, they must comply with the terms of the Data Use Agreement and this policy.

III. PROCEDURE

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

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

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

A limited data set may include only the following identifiers:

1. Dates, such as admission and discharge, service, and date of death. A patient's birth date should be Disclosed only if the University and the recipient of the information agree that it is needed for their purpose.
2. City, state, 5-digit zipcode; and
3. Ages in years, months, days, or hours

B. Data Use Agreements. A Data Use Agreement is required for use with limited data sets. All Data Use Agreements must be approved by the Office of Legal Counsel prior to execution. A Data Use Agreement must:

1. Establish the permitted Uses and Disclosures of the limited data set.
2. Establish who is permitted to Use or receive the limited data set.
3. Provide that the recipient of the information will:
    - Not Use or further Disclose the information other than as permitted by the Data Use Agreement or as Required by Law
    - Use appropriate safeguards to prevent Use or Disclosure of the information other than as permitted by the Data Use Agreement
    - Report to the University any Uses or Disclosures the recipient is aware of that are not provided for by the Data Use Agreement
    - Ensure that the recipient's agents who have access to the information agree to the same restrictions as imposed on the recipient
    - Not Use the information to identify or contact the individuals
    - Not Use or Disclose the information in a manner that would violate HIPAA if done by University Personnel.

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

IV. REFERENCES

A. HIPAA Privacy Regulations, 45CFR § 64.514 (e)

UNIVERSITY OF OKLAHOMA

HIPAA Policies

Title: Marketing	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Revised:** 2/1/2016; 4/1/2018

I. PURPOSE

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

II. POLICY*

A. Health Care Components must obtain an Authorization for any Use or Disclosure of Protected Health Information for Marketing purposes, **unless** the marketing communication is in the form of:

1) a face-to-face communication made by University Personnel to an individual; or
2) a promotional gift of nominal value provided by the Health Care Component and no payment was received for the activity.

(The University's Authorization for Marketing form may be used when Authorization is required.)

"Marketing" is defined as a communication about a product or service that encourages the purchase or use of the product or service. Using PHI (such as accessing patient addresses) for marketing is permitted if the marketing activity is a function of the Health Care Component's Health Care Operations.

Marketing does <u>not</u> include communications

- to provide refill reminders for current medications (if the HCC receives direct or indirect payment for sending the reminder, the payment may not exceed the reasonable cost to the HCC for sending it)
- for Treatment by a Health Care Provider, such as care coordination, and recommendations for alternate therapies or treatments, health care providers; or care settings (no payments may be received)
- for case management or care coordination or for contacting individuals about alternate treatment plans and related functions, to the extent they are not Treatment (no payments may be received)

If a Health Care Component or the University has received payment in exchange for A(1) or A(2) above, the activity is considered Marketing not Health Care Operations, unless;

(i) the communication describes only a drug or biologic that is currently being prescribed for the recipient of the communication and any payment is reasonable in amount;

(ii) the communication is made by the University and individual Authorization is obtained; or

(iii) the communication is made by a Business Associate on behalf of the University and the communication is made consistent with the Business Associate Agreement.

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

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

C. The University may not receive direct or indirect payment in exchange for Protected Health Information unless Authorized in writing by the individual. However, that general rule does not apply if the purpose of the payment is for:

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

III. PROCEDURE

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

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

IV. REFERENCES

A. HIPAA Privacy Regulations, 45 CFR 164.501
B. HIPAA Privacy Regulations, 45 CFR 164.508(a)(3)

UNIVERSITY OF OKLAHOMA

HIPAA Policies

Title: Mental Health Records, Substance Use Disorder Records, and Psychotherapy Notes	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Last Revised:** 4/1/2018

I. PURPOSE

To establish permitted Uses and Disclosures of mental health records, Substance Use Disorder Records, and Psychotherapy Notes, under state and federal law.

II. POLICY*

A. Mental Health and Substance Use Disorder Records – General

A patient generally has the right to access his/her mental health records **other than Psychotherapy Notes.** A patient can be denied access to his/her mental health records for one of the reasons set forth in the HIPAA *Patient Access to Own Protected Health Information* policy.

Mental health records and Substance Use Disorder Records receive more protection under Oklahoma and 42 CFR Part 2 law than under HIPAA. In accordance with HIPAA, then, Oklahoma and 42 CFR Part 2 law governs the privacy of these records. Mental health records, other than Psychotherapy Notes, may be Used and Disclosed to only those persons actively engaged in Treatment of the patient or related administrative work (such as scheduling). Mental health records may be Used or Disclosed only in accordance with the Minimum Necessary Rule, even for Treatment Purposes.

Persons or entities who want access to a patient's mental health records for purposes other than described above must obtain (1) an Authorization as required by the HIPAA *Authorization to Use or Disclose PHI* policy or (2) a valid court order.

The University may disclose mental health and Substance Use Disorder Records, subject to the Minimum Necessary Rule, for additional limited purposes:

- to carry out another provider's Treatment, Payment or Operations (excluding Substance Use Disorder Records);
- to Law Enforcement regarding crime on the premises or against University Personnel or a threat to commit such crime (with limited information on Substance Use Disorder patients);
- to review preparatory to research or research on decedents or for research conducted under a Privacy Board waiver;
- communicating under a Business Associate Agreement or Qualified Service Organization Agreement;
- reporting suspected child abuse or neglect to appropriate authorization (with no follow-up Disclosure permitted if the patient is a Substance Use Disorder patient);
- to medical personnel for purposes of treating a condition that poses an immediate threat

to others, requiring immediate medical intervention;

- for audit and evaluation activities;
- to obtain payment for services, if the Substance Use Disorder patient has a medical condition that prevents him from taking effective action on his own;
- reporting as otherwise Required by Law (but excluding the direct or indirect identity of a Substance Use Disorder patient);
- to communicate with coroners, medical examiners, and funeral directors to identify a deceased person or cause of death or to perform other duties (but excluding the direct or indirect identity of a Substance Use Disorder patient);
- to organ procurement organizations (but excluding the direct or indirect identity of a Substance Use Disorder patient);
- to a professional licensure board investigating alleged unethical behavior against a patient (but excluding the direct or indirect identity of a Substance Use Disorder patient);
- to the parent of a minor to notify of the minor's location (but excluding the direct or indirect identity of a Substance Use Disorder patient);
- to parties in personal injury or death cases against a provider (see 63 Okla. St. 1-1903);
- of consumer-identifying information if it appears the individual is an escapee, for purposes of identification and apprehension (but excluding all Substance Use Disorder Records);
- to prevent a serious threat to health or safety (but excluding the direct or indirect identity of a Substance Use Disorder patient).

The Office of Legal Counsel or the University Privacy Official should be contacted for assistance with responding to requests for mental health records or Substance Use Disorder Records.

NOTE: A subpoena alone is not sufficient for the release of mental health records. It must be accompanied by a HIPAA-compliant Authorization or a court order specifying the release of mental health records.

B. Psychotherapy Notes

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

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.

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

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

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

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

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

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

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

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

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

The Privacy Regulations do not permit a 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. (Additional HIPAA Health Plan policies are available on the HIPAA web page.)

C. Source Data

Only that PHI maintained in a Designated Record Set (see HIPAA *Definitions* policy) is required to be released. Source data interpreted or summarized in an individual medical record (example: pathology slide and diagnostic films) are not considered part of the Designated Record Set and therefore are not required to be released.

III. REFERENCES

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

UNIVERSITY OF OKLAHOMA

HIPAA Policies

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

I. PURPOSE

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

II. POLICY*

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

The Minimum Necessary Rule does not apply to:

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

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

Language such as the following should accompany requests for entire medical records: Based on my professional judgement, this request for the entire medical record is consistent with the Minimum Necessary Rule for the (describe) purpose intended.

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

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

III. PROCEDURE FOR AUTHORIZING APPROPRIATE LEVEL OF ACCESS TO PHI

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

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

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

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

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

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

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

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

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

Treatment should generally not have approved unlimited access to a patient's Protected Health Information -- access by these individuals is governed by the Minimum Necessary Rule.

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

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

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

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

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

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

IV. PROCEDURE FOR DISCLOSING PHI

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

B. Non-Routine Disclosures: Non-routine Disclosures of PHI (those that do not occur on a day-to-day basis as part of Treatment, Payment, or Health Care Operation activities or that are not Required by Law on a regular basis) shall not be made without first contacting the Office of Legal Counsel or the University Privacy Official. Examples include requests for PHI from state of federal agencies, search warrants, and media inquiries. The Office of Legal Counsel or University Privacy Official will give consideration to the following

criteria: (a) the purpose of the request; (b) any potential harm that would result to the patient, the University, or any other third party as a result of the Disclosure; (c) the relevance of the information requested; and (d) other applicable state and federal laws and regulations.

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

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

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

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

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

V. PROCEDURE FOR MAKING REQUESTS FOR PHI

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

B. Non-Routine Requests: Health Care Component managers and administrators must designate an individual who will be responsible for reviewing all non-routine requests (those that do not occur on a day-to-day basis as part of Treatment, Payment or Health Care Operation activities) for PHI. Any questions regarding the propriety or legality of a particular request must be submitted to the Office of Legal Counsel or the University Privacy Official, who will consider the following criteria: (a) the reason for the request; (b) any potential harm that would result to the patient, the University, or any other third party as a result of the Disclosure; (c) the relevancy of the information requested; and (d) other applicable state and federal laws and regulations.

VI. REFERENCES

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

UNIVERSITY OF OKLAHOMA

HIPAA Policies

Title: Mitigation	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Last Revised:** 4/1/2018

I. PURPOSE

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

II. POLICY*

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

III. PROCEDURE

A. Health Care Components must report to the University Privacy Official any instance of inappropriate Uses or Disclosures of or access to PHI. HCCs must, in coordination with the University Privacy Official or HIPAA Program Employees, take practicable steps to mitigate the harmful effects of inappropriate Use or Disclosure of Protected Health Information. The type of mitigation that occurs will be based on the facts and circumstances of each case, taking into consideration the following factors:

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

B. Health Care Components shall notify the University Privacy Official or HIPAA Program Employee, in accordance with the HIPAA *Complaint and Incident Reporting and Tracking* policy, of inappropriate Uses, Disclosures, and Access; the results of the investigation; and the proposed mitigation efforts. Once mitigation is determined, the Health Care Component must confirm it is implemented.

C. If legal action is threatened or is a distinct possibility as a result of the actual or suspected harmful effect despite mitigation efforts, the Health Care Component must notify the Office of Legal Counsel or University Privacy Official as soon as possible.

IV. REFERENCES

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

UNIVERSITY OF OKLAHOMA

HIPAA Policies

Title: Notice of Privacy Practices	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Last Revised:** 4/1/2018

I. PURPOSE

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

II. POLICY*

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

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

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

III. PROCEDURE

A. Acknowledgement of Receipt of Notice of Privacy Practices

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

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

B. Distribution of Notice of Privacy Practices

1. Request for Notice - University Health Care Components must make the Notice of Privacy Practices available to any person who requests it. The individual making the request does not have to be a patient of the University.

2. Direct Treatment Relationship - Health Care Components must ensure that Health Care

Providers with Direct Treatment relationships with patients do each of the following:

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

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

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

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

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

4. Indirect Treatment Relationship - Health Care Components with **Indirect** Treatment Relationships with patients must provide the Notice of Privacy Practices to individuals upon request.

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

C. Amendment of Notice of Privacy Practices

If the Notice of Privacy Practices is amended, the amended version must be posted and distributed to new patients. It also must be made available upon request to current patients. (See HIPAA *Development and Amendment of HIPAA Policies, Procedures, and Forms* policy.)

D. Retention

Each version of the Notice of Privacy Practices must be retained by the University Privacy Official for six years.

IV. REFERENCES

A. HIPAA Privacy Regulations, 45 CFR 164.520

UNIVERSITY OF OKLAHOMA

HIPAA Policies

Title: Personal Representative	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Last Revised:** 4/1/2018

I. PURPOSE

To establish who can act on behalf of adult, minor, and deceased patients for purposes of Authorizing Uses and Disclosures of PHI and exercising the patient's rights under HIPAA.

II. POLICY*

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

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

A. Personal Representatives for Adults

Adults can act as a Personal Representative of another adult (or of a person under 18 who may legally consent to health services) if they possess documentation of any of the following, in the order of priority:

1. 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 but must include the authorization to make personal medical decisions.

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

The appointment of the Health Care Proxy may be completely or partially revoked at any time and in any manner by the patient. A revocation is effective when the patient communicates the desire to revoke to the attending physician or other University Personnel. If the patient revokes the advanced directive, the Health Care Proxy no longer qualifies as a Personal Representative. The Provider or University Personnel receiving notice of the revocation must note the revocation in the patient's medical record or inform the medical records department.

3. Durable Power of Attorney for Health Care. A durable power of attorney is a document the patient uses to designate an individual as his agent to perform certain acts on his behalf. Under a valid durable power of attorney, and *depending on the scope of the power of attorney,* the agent may make health and medical care decisions on the patient's behalf.

Note: A Durable Power of Attorney does not give the agent the power to execute an advance directive for health care, living will, or other document to authorize life-sustaining treatment decisions or to make life-sustaining treatment decisions unless the power of attorney complies with the requirements for a Health Care Proxy. Contact the Office of Legal Counsel for assistance.

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, incapacity, or extended absence of the principal or lapse of time,*" or "*This power of attorney shall become effective upon disability, incapacity, or extended absence of the principal,*" or similar words showing the intent of the patient that the power of attorney will be exercisable even in cases of the patient's subsequent disability, incapacity, or extended absence of the principal or lapse of time. The document must state whether the power is effective when the patient is competent or only once the patient becomes incompetent.

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

4. Patient's Spouse;

5. Adult Children of the Patient;

6. Parents of the Patient;

7. Adult Siblings;

8. Other Adult Relatives of the Patient in Order of Kinship; or

9. Close Friends of the Patient – Those who have maintained regular contact with the patient sufficient to be familiar with the patient's personal values. Execution of an affidavit stating specific facts and circumstances documenting such contact constitutes sufficient evidence of close friendship.

B. Personal Representatives for Experimental Treatment

Individuals Designated in Experimental Treatment Statute. The Oklahoma Experimental Treatment statute, 63 Okla. Stat. 3102A, provides that a legal guardian, attorney-in-fact, and

certain enumerated family members may consent to an incapacitated adult patient's participation in a research study being conducted by a University faculty member who has received IRB approval for the study. Contact the Human Research Participant Protection office for assistance.

C. Personal Representatives for Minors

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

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

a. The minor is married, has a dependent child, or is emancipated.

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

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

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

e. The minor is not able to give consent due to reason of physical or mental capacity and has no known relatives or legal guardian, and two physicians agree on the health service to be given.

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

In addition, the minor's spouse may give consent if the minor is incapable of consenting because of physical or mental incapacity.

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

Except as set forth in paragraph C(1)(c) above, University Personnel are required to make a reasonable attempt to inform the spouse, parent, or guardian of the minor of any emergency services provided to the categories of minors set forth above. In all other instances, University

Personnel may, but are not required to, inform the spouse, parent, or legal guardian of the minor of any treatment provided.

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

D. Personal Representatives for Deceased Individuals

If under applicable law there is an executor, administrator, or other person having authority to act on behalf of a deceased individual or of the individual's estate, that individual must be treated as the Personal Representative of the deceased, with respect to PHI, and may Authorize the Use or Disclosure of the deceased patient's Personal Health Information. The court document appointing the individual as an executor or administrator is known as the Letters Testamentary or Letters of Administration and is signed by a judge.

Under Oklahoma law, the following individuals have authority to act as a Personal Representative of a deceased individual if there is no executor or administrator appointed: the spouse of the deceased or, if no spouse, any responsible family member of the deceased. A responsible family member is a parent, adult child, adult sibling, or other adult relative of the deceased who was actively involved in providing or monitoring the care of the deceased, as verified by the doctor, hospital, or other medical institution that was responsible for providing care and treatment of the deceased.

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

III. PROCEDURES

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

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

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

IV. REFERENCES

A. 58 Okla. Stat. 1072.1
B. 63 Okla. Stat. 3101.1., 3102 et. seq.
D. 63 Okla. Stat. 2602
E. 30 Okla. Stat. 3-112
F. 76 Okla. Stat. 19
G. HIPAA Privacy Regulations, 45 C.F.R. 164.502 (g)

UNIVERSITY OF OKLAHOMA

HIPAA Policies

Title: PHI in Research	**Approved:** March 8, 2012
Effective Date: March 8, 2012	**Last Revised:** 4/1/2018

I. PURPOSE

To establish permitted Uses and Disclosures of PHI in Research and requirements for protecting Research-related PHI.

II. POLICY*

A Health Care Component may Use and Disclose PHI for the purposes of Research only in accordance with University's Office of Human Research Participant Protection (HRPP) policies, including the HRPP HIPAA Policies. The University's Institutional Review Board shall serve as the University's Privacy Board.

"Research" is defined under HIPAA as a systematic investigation -- including research development, testing, and evaluation -- designed to develop or contribute to generalizable knowledge.

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

a. Authorization for the Use of Disclosure of PHI;
b. Waiver of the Authorization requirement by the Privacy Board;
c. De-identification of the PHI in accordance with the HIPAA *De-Identification/Re-Identification of PHI* policy; or
d. Use of a Limited Data Set, with accompanying Data Use Agreement (available on the HIPAA forms webpage and from the HRPP Office.)

Authorizations must comply with the HIPAA *Authorization to Use or Disclose PHI* policy and applicable HRPP policies.

III. PROCEDURE

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

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

C. Research involving the Use or Disclosure of De-Identified Health Information or Limited Data Sets must comply with HRPP policies as well as HIPAA *Limited Data Set* policy, and HIPAA *De-Identification/Re-Identification of PHI* policy.

D. Persons conducting Research involving PHI are responsible for logging Disclosures, pursuant to the HIPAA *Accounting of Disclosures* policy.

E. Any violations of the University's HIPAA policies during the course of Research must be reported to the HRPP office and the University Privacy Official as soon as possible, in compliance with the HIPAA *Complaint and Incident Reporting and Tracking* and *Breach of Unsecured PHI/ePHI* policies. Examples of HIPAA violations that may arise in Research include **but are not limited to**:

1. Failure to obtain a signed Authorization
2. Sharing PHI with individuals or entities not listed on the Authorization or permitted under the HIPAA Regulations.
3. Storing PHI on unencrypted devices or in unapproved cloud storage.
4. Failing to secure paper or electronic copies of PHI.
5. Emailing PHI via unencrypted transmission.

IV. REFERENCES

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

UNIVERSITY OF OKLAHOMA

HIPAA Policies

Title: Protecting ePHI From Improper Alteration or Destruction	**Approved:** January 2, 2014
Effective Date: January 2, 2014	**Last Revised:** 4/1/2018

I. PURPOSE

To describe the procedures that must be in place to protect each Health Care Component's ePHI from improper or unauthorized alteration or destruction.

II. POLICY*

Each Health Care Component, in coordination with IT Security and the HIPAA Security Officer, shall have in place Technical Safeguards to protect the ePHI it maintains on its Information Systems from improper or unauthorized alteration or destruction.

III. PROCEDURE

A. As part of its Technical Safeguards, each Health Care Component must protect its ePHI from improper or unauthorized alteration or destruction by ensuring the following:

1. All access to ePHI must require the User to Authenticate -- such as by password -- to the Information System. The HCC shall comply with the IT information access policies and procedures applicable to the HCC's campus and with this Policy.
2. Each HCC must establish or utilize, in coordination with its Tier 1 or IT Representative, Technical Safeguards to corroborate that its ePHI has not been improperly altered or destroyed. At a minimum, the HCC shall follow the IT technical safeguards established for access on its campus and in the HIPAA *Technical Safeguards* policy.
3. Each HCC must have a process in place to verify that the person or entity seeking Access to the HCC's ePHI is who he claims to be.
    a. Each HCC must comply with its campus IT password management policy and ensure that its Workforce Members receive training or written instruction for properly managing their passwords.

        At a minimum, the IT password management policy must:

        i. Prohibit sharing passwords

        ii. Allow Workforce Members to select and change their own passwords

        iii. Require passwords that meet the standards defined by the HCC's

campus IT Department

iv. Require regular password changes

v. Not display passwords in clear text when they are being input

vi. Require that passwords be stored only in an encrypted form

vii. Require secure delivery of passwords to Users

viii. Require that default vendor passwords be reset upon installation of software or hardware

ix. Require that temporary passwords be randomly generated, and force password change at first log-on, when possible

b. The password management training awareness program provided by IT and/ or the HIPAA Security Officer or written instruction provided by the HCC manager must require users to comply with the following:

i. Keep passwords confidential

ii. Avoid keeping a paper record of passwords, unless the record is stored securely

iii. Change passwords when compromise to the system or password may have occurred

iv. Comply with IT's password standards

v. Not use the same password for personal and business accounts

vi. Change passwords regularly; do not reuse passwords

vii. Change temporary passwords at first log-on

viii. Do not include passwords in automated log-on processes (e.g., storing in a browser or function key)

ix. Understand that activities involving their user name and password will be attributed to them.

4. Encryption and Decryption of ePHI

a. ePHI must be encrypted when stored outside of the campus enterprise data center (such as on local servers or devices).
b. ePHI sent via email to authorized recipients must be encrypted. (See HIPAA *Emailing and Transmitting PHI* policy and HIPAA *Administrative and Physical Safeguards* policy).
c. The HCC must have a way to decrypt any ePHI that it encrypts or has encrypted.

B. Each HCC shall, in coordination with Information Technology and the HIPAA Security Officer, configure or enable its hardware, software, and/or procedural mechanisms to record for HCC examination the User activity in its Information Systems that contain ePHI. Reviews must be handled in accordance the HIPAA *Access to ePHI Systems* policy.

If improper activity is observed by the HCC manager, the manager shall immediately report it to IT Security, the HIPAA Security Officer, or the University Privacy Official.

IV. Health Care Components must comply with all Information Technology policies designed to protect Information Systems that maintain ePHI.

V. REFERENCES

A. 45 CFR 164.312(c)-(e)
B. Applicable Information Technology Policies
C. HIPAA Access to ePHI Systems Policy
D. HIPAA Administrative and Physical Safeguards policy
E. HIPAA Technical Safeguards policy

UNIVERSITY OF OKLAHOMA

HIPAA Policies

Title: Purchasing or Leasing Equipment or Contracting for Services Involving PHI	**Approved:** June 15, 2016
Effective Date: June 15, 2016	**Last Revised:** 4/1/2018; 12/18/2018

I. PURPOSE

To ensure that equipment and services that HCCs use that involve the receipt, storage, or transmission of University PHI do not put University PHI or systems at an unacceptable level of risk for compromise and appropriately document the service provider's responsibilities.

II. POLICY*

A. External Vendors/Providers. Health Care Components that purchase or lease equipment or acquire technology or services that receive, store, or transmit PHI must comply with University Purchasing and IT Security R.I.S.K. Program policies, described below.

This Policy applies to but is not limited to purchases, leases, and contracts for services related to software, transmission services, network printers and copy machines, cloud storage, medical equipment and devices, computing devices, and technology services. This Policy applies regardless of the dollar amount of the transaction and regardless of how the transaction will be billed or paid.

Small dollar and P-card purchases are subject to this policy. Sole source purchases are subject to this policy.

1. Equipment/Software: Prior to purchasing or leasing the equipment or software described above, Health Care Component managers or administrators must contact IT Security and ask that a review of the product's security features and risks be completed. IT Security will evaluate the security features and issue recommendations regarding how to address or mitigate any risk identified, such as by implementing a technical control for the product (the R.I.S.K. Program). Health Care Components are expected to comply fully with Information Technology's recommendations prior to using the equipment or software or to obtain written administrative approval to do otherwise.

   Health Care Component managers or administrators must inform the Purchasing Department if the equipment/software will be used for PHI so Purchasing can obtain a Business Associate Agreement if appropriate.

   Health Care Component managers or administrators must also inform the Purchasing Department if leased equipment or software will be used for PHI, so that Purchasing can ensure the leasing agreement (or Request for Proposal or Bid, as appropriate) includes a requirement that the vendor destroy or wipe the hard drive in a manner that complies with

HIPAA when the lease term ends and the vendor takes possession of the leased equipment or that permits the University to do so.

2. Services: Prior to contracting for the services described above, Health Care Component managers or administrators must inform the Purchasing Department that the services will involve the University's PHI, so that Purchasing can include Business Associate terms in the agreement with the service provider.

   If the services include the service provider accessing or using University servers or IT systems, the Health Care Component manager or administrator also must request that IT Security review the proposed access and make a recommendations regarding how to address any risk identified, such as by implementing a technical control for the vendor's access to the server or system (the R.I.S.K. program). Health Care Component managers are expected to fully comply with Information Technology's recommendations or to obtain written administrative approval to do otherwise.

3. Managed Services. If the services acquired are managed services that may impact the University's PHI, such as maintenance or administration of servers, devices, equipment, or information or technology systems that store, process, transmit, or provide for the protection of the University's PHI -- regardless of who owns the system(s) involved -- the Health Care Component manager or administrator must request that IT Security review and make recommendations regarding the proposed access and the adequacy and specificity of the responsibilities assumed by the service provider (the R.I.S.K. program). Health Care Component managers are expected to fully comply with Information Technology's recommendations or to obtain written administrative approval to do otherwise.

   If the services include access to the University's electronic medical or billing record systems, the Health Care Component shall not permit such access until the vendor has completed the required HIPAA *Terms of Access to PHI/ePHI* forms (see the HIPAA Forms page).

   The Health Care Component manager or administrator must inform the Purchasing Department that the services will involve University PHI, so that Purchasing can include Business Associate terms in the agreement with the service provider.

B. Internal Vendor/Providers. If the equipment or services will be provided by an internal University department, such as Information Technology, IT Security, or Printing Services, the Health Care Component must have in place a written document that specifies who is providing what equipment and/or service, that PHI is involved and must be maintained in confidence, and what specific services and/or equipment is being provided.

C. Health Care Components may contact the Purchasing Department, IT Security, the University Privacy Official, or the HIPAA Security Officer if they have questions regarding these requirements.

D. If equipment or services are acquired through a contract managed by another office, such as the Office of Research Administration or Office of Research Services, that office shall be responsible for the actions attributed to Purchasing above.

III. REFERENCES

A. 45 CFR 164.306
B. Board of Regents Policy, 4.11, Buying and Selling Goods and Services
C. Purchasing Department Small Dollar Policy
D. Information Security R.I.S.K. Program Policy

UNIVERSITY OF OKLAHOMA

HIPAA Policies

Title: Request to Amend Records	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Last Revised:** 4/1/2018

I. PURPOSE

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

II. POLICY*

The University will permit patients to request amendments or corrections to their Protected Health Information contained in a Designated Record Set. (See HIPAA *Definitions* policy.)

A. The University may deny a patient's request for amendment or correction 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 individual who created the Protected Health Information is no longer available to act on the request;

2. is not part of the Designated Record Set;

3. is not available for inspection by the patient (See *Patient Access to Own Protected Health Information* policy); or

4. is accurate and complete.

B. Patients requesting to amend or correct their Protected Health Information must provide a reason to support the request using the HIPAA *Request to Amend PHI* form, available on the HIPAA website.

C. 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 the HCC's Designated Record Set.

III. PROCEDURE

A. Patients must request amendments to their Protected Health Information in writing by using the University's HIPAA *Request to Amend Protected Health Information* form. Health Care Components that receive a Request to Amend by telephone or e-mail must send the patient a copy of the form or refer the patient to the HIPAA forms for patients webpage. Verification of

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

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

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

The specific provider responsible for recording the Protected Health Information or originating the record must be consulted, if possible, and should sign the Request form.

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

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

2. Denying the Request. If the Health Care Component denies the request, in whole or in part, the Health Care Component must: (a) inform the patient, in writing, that the change is denied by sending the patient a copy of the Denial form; (b) permit the patient to submit to the Covered Entity a written statement disagreeing with the denial of all or part of a requested change and the basis of such disagreement; (c) identify, as appropriate, the record or Protected Health Information in the Designated Record Set that is the subject of the disputed request and append or otherwise link the patient's request; 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 must be provided to the patient who submitted the statement of disagreement.) The University Privacy Official must be contacted prior to sending the rebuttal.

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

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

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

IV. REFERENCES

A. HIPAA Regulations, 45 CFR 164.526 (a)

UNIVERSITY OF OKLAHOMA

HIPAA Policies

Title: Retaliation and Intimidation	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Last Revised:** 4/1/18

I. PURPOSE

To prohibit retaliation and intimidation against individuals who exercise their rights under HIPAA.

II. POLICY*

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

A. Exercising any right under, or for participating in, any process established by HIPAA;

B. Filing a complaint with the University Privacy Official, Office of Compliance, HIPAA Program Employees, or the Secretary of the Department of Health and Human Services or other entity, as permitted by the HIPAA Regulations;

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

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

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

III. PROCEDURE

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

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

*Capitalized items are defined in HIPAA *Definitions* policy

C. If the individual believes the University Privacy Official has retaliated against or intimidated him, the individual should report the incident to the University's Director of Compliance at 405-271-2511, the Compliance anonymous hotline at 866-836-315, or the General Counsel at 405-325-4124 for investigation and sanction, if warranted. If the individual believes the Office of Compliance has retaliated against or intimidated him, the individual should report the incident to the General Counsel.

IV. REFERENCES

A. HIPAA Regulations, 45 CFR 164.530(g)
B. HIPAA Regulations, 45 CFR 160.316
C. HIPAA Administrative Regulations, 45 CFR 160.316

UNIVERSITY OF OKLAHOMA

HIPAA Policies

Title: Right to Request Restriction on Use and Disclosures	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Last Revised:** 4/1/2018

I. PURPOSE

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

II. POLICY*

A. Health Care Components will permit patients to request restrictions on the Use and Disclosure of their Protected Health Information: (1) to carry out Treatment, Payment, or Health Care Operations and/or (2) to people involved in their care or for notification purposes (See HIPAA *Disclosures to Family and Others Involved in Patient's Care* policy). **However, an HCC is not <u>required</u> to agree to any request to restrict the Use and Disclosure of Protected Health Information, unless the Disclosure is to a Health Plan for purposes of Payment or Health Care Operations; <u>and</u> the PHI pertains to a health care item or service for which the patient or individual on behalf of the patient (such as a family member) has paid the University in full.**

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

Any agreed-upon restriction will not be effective to prevent Uses and Disclosures to the patient.

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

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

III. PROCEDURE

A. Patients must request restrictions on the Use and Disclosure of their Protected Health Information in writing by using the HIPAA *Request for Restriction on Use and Disclosures of Protected Health Information* form. Health Care Components shall send a copy of the form to patients making their restriction requests by telephone or e-mail or refer them to the HIPAA

forms for patients webpage. Verification of the requester's identity must be obtained prior to considering the request. (See HIPAA *Verification of Identification* policy.)

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

C. Health Care Components must designate and document the title(s) of the individual or office responsible for receiving and processing Request for Restriction forms. A copy of the designations must be provided to the University Privacy Official or designee upon request. The Health Care Components must update the list as changes are made and provide the updated list to the University Privacy Official upon request. The Health Care Component will maintain a copy of the designation for a minimum of six (6) years.

Requests for restrictions that are not required to be granted should generally be granted when facts and circumstances indicate such a restriction is necessary to protect the patient.

D. The Privacy Official may be contacted for assistance prior to agreeing to or denying any restriction request.

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

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

G. The agreed-upon restrictions should be communicated to the billing department and other departments, providers, and Business Associates who may be Using or Disclosing the patient's Protected Health Information on behalf of the University and/or Health Care Component that agreed to the request. Health Care Components should send those departments and entities a copy of the approved Request form.

H. A restriction that has been granted but is not Required by Law can be terminated if (1) the patient requests the termination in writing; (2) the patient orally agrees to or requests the termination and the oral request or agreement is documented in the patient's medical record and communicated in writing to the University Privacy Official; or (3) the University and/or the Health Care Component informs the patient that it is terminating its agreement to the voluntary restriction, in which case the termination will apply only to Protected Health Information created or received after the patient has been notified of the termination. The HIPAA *Revocation of*

Request for Restriction and Use and Disclosure of PHI form, available on the HIPAA website, may be used.

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

IV. REFERENCES

A. HIPAA Regulations, 45 CFR 164.522 (a)

UNIVERSITY OF OKLAHOMA

HIPAA Policies

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

I. PURPOSE

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

II. POLICY*

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

This policy establishes minimum administrative and physical standards regarding the protection of PHI that each Health Care Component must enforce, as applicable. Health Care Components may develop additional policies and procedures that are stricter than the those in this Policy to address the unique circumstances of a particular Health Care Component but may not do less than is required by this policy. Policies and procedures developed in addition to these will be reviewed by the University's Privacy Official and Security Officer upon request.

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

B. Health Care Components may Disclose PHI to other components of the University that are not designated Health Care Components only with patient Authorization or as permitted or Required by Law.

University Personnel who perform services for Health Care Components and for other components of the University must not otherwise Use or Disclose PHI created or received in the course of or incident to their work for the Health Care Component to components of the University that are not Health Care Components.

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

A. Administrative Safeguards.

1. Oral Communications. University Personnel must exercise care to avoid unnecessary Disclosures of PHI during oral communications. For example, voices should be quiet and

conversation should not occur if unauthorized individuals are present. Patient identifying information should be Disclosed during oral conversations only when necessary for Treatment, Payment, teaching, Research, or Healthcare Operations purposes. Dictation and telephone conversations must be conducted away from public areas if possible. Office doors should be closed when PHI is being discussed. Speakerphones may be used only in private areas.

2. Telephone Messages. Telephone messages and appointment reminders *that do not contain PHI* may be left on answering machines and voice mail systems, unless the patient has requested and received approval for an alternative means of communication (See HIPAA *Communication by Alternative Means* policy.) Telephone messages that contain information that links a patient to a particular medical condition, diagnosis, or treatment must be avoided, unless the patient has provided written Authorization to receive PHI in telephone messages.

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

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

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

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

c. Unless otherwise permitted or Required by Law, a properly completed and signed Authorization must be obtained before faxing PHI to third parties (including faxes to University departments that are not designated Health Care Components) for purposes other than Treatment, Payment, or Health Care Operations. (See HIPAA *Authorization to Use or Disclose PHI – Other Than to Patient* policy.)

d. All faxes containing PHI must be accompanied by a cover sheet that includes a confidentiality notice. PHI may not be included on the cover sheet. A sample fax cover sheet with the confidentiality notice is available on the HIPAA Forms webpage.

e. Reasonable efforts must be made to ensure that fax transmissions are sent to the correct destination. Frequently used numbers should be programmed into fax machines or computers to avoid dialing errors. Programmed numbers should be verified on a regular basis. The numbers of new recipients should be verified prior to first transmission.

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

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

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

4. Mail. PHI may be mailed within the University if placed in a sealed envelope or in a locked mail bag. PHI, including appointment reminders, may be mailed outside the University if the contents are concealed and the envelope is sealed. The return address may not indicate the nature of diagnosis, treatment, or condition.

5. Copies. All copies of PHI provided to the patient or another third party in response to a request for access should be date-stamped in a color other than black or should havce some other unique identifying mark or symbol, so that a copy can be distinguished from the original.

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

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

7. Destruction Standards. PHI must be discarded in a manner that protects the Confidentiality of the information. Paper and other printed materials containing PHI must be destroyed or cross-cut shredded so that they cannot be read or reconstructed. Health Care Components may also obtain and use locked recycling bins from one of the University's approved recycling vendors. Magnetic media and disks containing PHI must be overwritten or reformatted if possible or shredded or otherwise destroyed pursuant to industry standards (available from IT Security.) Hard drives and other electronic devices must be destroyed or managed in accordance with applicable IT Security policies. (Additional information is available from IT Representatives/ Tier 1s.)

B. Physical Safeguards.

1. Paper Records. Documents containing PHI must be stored or filed in such a way as to avoid access by unauthorized persons. Some type of reasonable secure physical barrier must be used to protect paper records from unauthorized access. Documents containing PHI on attended desks, counters, or nurses' stations must be placed face down or positioned in a manner that prevents access by unauthorized persons. Paper records shall be secured when the area is unattended.

a. Storage. Paper records that contain PHI and are stored outside of the Health Care Component must be inventoried and stored in a secure, University-approved facility. The Health Care Component shall maintain a log of who has access to the stored records and

have in place a procedure for terminating access when employment ends. (See, *Procedures for Storing Protected Health Information* on the HIPAA FAQ page.)

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

The security and return of the documents checked out or removed are the sole responsibility of the person who removed them. Documents containing PHI that are removed from University premises must not be left unattended in places in which unauthorized persons can gain access, legally or otherwise. They must not be left unattended in the passenger compartment of automobiles, for example, or in common areas.

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

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

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

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

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

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

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

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

III. REFERENCES

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

UNIVERSITY OF OKLAHOMA

HIPAA Policies

Subject: Safeguards - Technical	**Approved:** January 2, 2014
Effective Date: January 2, 2014	**Last Revised:** 4/1/2018

I. PURPOSE

To describe the Technical Safeguards that must be in place to protect each Health Care Component's ePHI from unauthorized Access and Use. (See also HIPAA *Protecting ePHI from Improper Alteration or Destruction* policy.)

II. POLICY*

Each Health Care Component, in coordination with Information Technology and the HIPAA Security Officer, shall have in place Technical access and audit controls, including encryption of portable electronic devices used for University Business, to protect the ePHI it maintains on its Information Systems from unauthorized Access or Use.

III. PROCEDURE

A. As part of its Technical Safeguards, each Health Care Component shall comply with or provide for the following:

1. Computer Logoff/Lock Policy - HCC administration and the HCC's assigned Tier 1 or IT Representative shall enforce both of the following requirements for computer lock and logoff:
   a. Lock – Workforce Members must manually lock or log off a computing device or application when leaving that device or application unattended, even for brief periods.
   b. Automated Lock or Logoff – All computing devices and applications must be secured with either a password-protected screen saver or automatic log off that will take effect after the time period established by IT Security, currently no more than 15 minutes of inactivity.

2. Encryption and Decryption of ePHI, as described in the HIPAA *Protecting ePHI from Improper Alteration or Destruction* policy.

Workforce Members must comply with the HIPAA policies regarding emailing PHI to patients (See HIPAA *Emailing and Transmitting PHI* policy), as well as with the policy or practice of their HCC. For OU Physicians, for example the preferred method for communicating electronically with patients is through a secure patient portal.

B. Each HCC shall, in coordination with Information Technology and the HIPAA Security Officer, configure or enable its hardware, software, and/or procedural mechanisms to

record for examination the User activity in its Information Systems that contain ePHI to the extent technology is available. Reviews of the records shall be handled in accordance the HIPAA *HCC Review of Access to ePHI Systems* policy and related University audit policies. If improper access is observed by the HCC manager, it shall be immediately reported to the University Privacy Official or HIPAA Security Officer.

C. IT representatives and Tier 1s who put University-owned, University-leased, or personally-owned portable devices into service must encrypt the device prior to releasing it for use. Workforce Members who put such devices into service for University Business without the assistance of IT must have their Tier 1 or IT Representative encrypt the device prior to using for University Business.

D. Health Care Components, with assistance from their Tier 1 or IT Representative, must comply with all Information Technology and related policies designed to protect Information Systems that maintain ePHI, including but not limited to maintaining anti-virus software on all devices and equipment that create, transmit, or store PHI.

IV. REFERENCES

A. 45 CFR 164.312(a) – (b)
B. Information Technology Password Management Policy and Standards
C. Information Technology Transmission of Sensitive Data Policy
D. Information Technology Computer Logoff/Lock Policy
E. Information Technology Activity (Log) Review Policy
F. HIPAA Audits Policy
G. HIPAA Compliance Audit Program policy
H. HIPAA Administrative and Physical Safeguards policy
I. HIPAA Protecting ePHI from Improper Alteration or Destruction policy

UNIVERSITY OF OKLAHOMA

HIPAA Policies

Title: Sanctions	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Last Revised:** 4/1/2018

I. PURPOSE

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

The purpose of this Policy is to establish a framework for sanctions to address HIPAA violations by OU Workforce Members and Business Associates.

II. POLICY*

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

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

III. PROCEDURE

Health Care Components shall follow the guidance below in evaluating whether sanctions are appropriate for HIPAA violations and, if so, for implementing those sanctions. If an HCC establishes its own sanctions policy, it must be consistent with these guidelines.

Documentation regarding any sanction imposed for a violation of the HIPAA Policies or Regulations shall be retained by the Health Care Component and if appropriate, 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 shall be forwarded to the University Privacy Official upon request, who also shall maintain such documentation for at least six (6) years.

A. Sanctions Against Business Associates. If the University, through the University Privacy Official, determines that a Business Associate's pattern of activity or practice constitutes a material breach or violation of the Business Associate's obligations under HIPAA or under its Business Associate agreement with the University, then the University Privacy Official:

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

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

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

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

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

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

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

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

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

1. **Category 1: Accidental or Inadvertent Violation or Failure to Follow HIPAA Privacy and Security Policies and Procedures.** This category includes unintentional violations of HIPAA caused by carelessness, lack of training, or human error, as well as violations due to poor job performance or lack of performance improvement. Examples of Category 1 violations include:
    a. Inadvertently accessing or releasing PHI without a written Authorization that complies with University policy and applicable law;
    b. Directing PHI via mail, e-mail, or fax to the wrong recipient(s)
    c. Giving a clinic visit summary, lab result, or similar, to the wrong patient

d. Failing to Safeguard documents containing PHI
e. Leaving PHI on an answering machine/voicemail or discussing PHI in a public area;
f. Failing to report HIPAA violations the Workforce Member causes, observes, or has knowledge of;
g. Improperly disposing of PHI;
h. Failing to properly sign off from or lock computer when leaving a work station unattended;
i. Failing to properly safeguard password or log-in credentials;
j. Failing to safeguard a portable device or the PHI on an electronic device from unauthorized access, loss, or theft;
k. Transmitting PHI via an unsecured method

2. **Category 2: Deliberate or Purposeful HIPAA Violation But Without Harmful Intent.** This category involves a second offense or an intentional violation due to curiosity, desire to gain information, or for personal or improper use. Examples of this type of violation include:
    a. Second offense of any Class I offense (does not have to be the same offense);
    b. Accessing, Using, or Disclosing PHI without a legitimate need to do so, such as an employee checking his own medical record, reviewing the results of a coworker's lab work, or accessing a family member's or friend's record outside of the employee's job responsibilities;
    c. Posting PHI on a social media or similar act;
    d. Removing PHI from the premises solely for convenience and without proper approval;
    e. Sharing or using shared access codes or log-in credentials;
    f. Failing to cooperate with authorized individuals in the investigation, mitigation, or resolution of a HIPAA incident;
    g. Failing to complete the University's mandatory annual HIPAA training in a timely manner
3. **Category 3: Willful and Malicious Violation or Violation with Harmful Intent.** This category includes a repeat offense or an intentional violation causing or likely to cause harm to a patient or the University. Examples of this type of violation include:
    a. Repeat of any Class I or II offense (does not have to be the same offense);
    b. Disclosing PHI to an unauthorized individual or entity for illegal or illicit purposes (e.g., identity theft, fraud);
    c. Creating or modifying PHI for unauthorized or improper purposes or under false pretenses;
    d. Disclosing a patient's PHI to the media;
    e. Obtaining PHI under false pretenses

E. Sanctions Against Employees by Category. Once the manager or individual imposing the sanction has determined the category of offense, the sanction(s) imposed should be consistent with the following, unless mitigating factors exist and are documented.
1. Category 1 - Sanctions for Category 1 offenses may include, but are not limited to:
    a. Termination of employment;
    b. Suspension for a stated suspension period, generally one to three days;

c. Retraining on the proper use of HIPAA forms and/or policies and procedures, as appropriate;
d. Written reprimand maintained in employee's personnel file permanently;
e. Informal verbal counseling/reprimand;
f. Verbal counseling/reprimand, documented in the investigation file and, if appropriate, the personnel file permanently

2. Category 2– Sanctions for Category 2 Offenses may include, but are not limited to:
    a. Termination of employment;
    b. Suspension for a stated period, generally one to three days;
    c. Retraining on proper use of HIPAA forms and/or policies and procedures, as appropriate;
    d. Written reprimand maintained in the investigation file and in the employee's personnel file permanently
3. Category 3 – Sanctions for Category 3 Offenses may include, but are not limited to:
    a. Termination of employment/abrogation of tenure (administered in conformance with the OUHSC Faculty Handbook, including, Section 3.16 "Abrogation of Tenure, Termination of Employment, Severe Sanctions; Summary Suspension; and Other Disciplinary Actions Imposed for Failure to Comply with The University Compliance Program, Professional Practice Plan Billing Compliance Policy, or Other Federal or State Mandates");
    b. Extended period of suspension, generally four to five days

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

VI. MITIGATING FACTORS

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

- Violation of sensitive PHI such as HIV, psychiatric, substance abuse, or genetic data
- High number of people or volume of data affected
- High exposure (e.g., financial, reputational) for the University
- Large University or HCC expense incurred, such as for breach notifications or mitigation
- Hampering the investigation; lack of truthfulness or cooperation
- Violator's level of training in HIPAA (e.g., inadequate training, training barriers)
- Culture of surrounding environment (e.g., investigation determines inappropriate practices in business unit with manager's knowledge or direction)
- Victim(s) suffered no financial, reputational, or other personal harm and risk of compromise of PHI is low, as determined by University Privacy Official's risk assessment
- Violator voluntarily reported the violation in a timely manner and cooperated with the investigation

- Violator showed remorse and accepted responsibility for the violation
- Frequency with which the violator accesses or Uses PHI as part of her job responsibilities
- Violation action was confirmed to have been taken under pressure from an individual in a position of authority
- Time between offenses

V. REFERENCES

A. HIPAA Privacy Regulations, 45 CFR 164.530(e)(1)
B. HIPAA Security Regulations, 45 CFR 164.312(e)

UNIVERSITY OF OKLAHOMA

HIPAA Policies

Title: Tracking, Returning, and Disposing of Device and Media	**Approved:** January 2, 2014
Effective Date: January 2, 2014	**Last Revised:** 4/1/2018

I. PURPOSE

To establish requirements regarding tracking devices and media that contain ePHI into, out of, and within the Health Care Component's facility.

II. POLICY*

Each Health Care Component must develop and implement procedures that govern the receipt and removal of hardware and electronic media that contain PHI, into and out of their assigned primary locations. University-owned and University-leased hardware and electronic devices that create, store, or transmit PHI and that are intended for use primarily on University property may not be removed from University property without supervisor approval.

Note: Tracking the movement of devices that are intended to be portable, such as laptops and flash drives, is not required. However, such devices are to be included on the HCC's Device Inventory. A copy of the Health Care Component's device and media control procedures shall be provided to HIPAA Program Employees upon request.

III. PROCEDURE

Each Health Care Component's device and media control procedures must address, at a minimum, the following:

A. Accountability for Devices and Media — To ensure the Health Care Component has a current tracking system, each HCC manager must designate an individual, such as the HCC's Tier 1 or Technical Representative, to maintain an inventory of University-owned, University-leased, and personally-owned devices and media that are used by HCC Workforce Members for University Business, including medical devices. The designated individual may be or may maintain the inventory in coordination with the Health Care Component's Tier 1 or IT Representative, as applicable.

1. The designated individual shall perform a reconciliation of the inventory regularly, typically no less than annually. Reconciliation should include University-owned, University-leased, and personally-owned devices and media used for University Business, including those being used at off-campus locations.

2. The inventory shall contain, at a minimum;
   a. Type of device

b. Primary location
c. Description
d. Role
e. Who device is issued to
f. Identifying serial number or asset tag ID number
g. Encryption status
h. Disposition of device

This inventory may be combined with the destruction log, described in B(2)(d) below.

A sample inventory log is attached to this policy and is available on the HIPAA website or from the HIPAA Security Officer.

B. Disposition of Devices and Media

1. Re-Use Procedures – Each HCC must implement procedures for removal of PHI from electronic media before the media is made available for re-use. The procedure shall include:

   a. If a Workforce Member is no longer authorized to use the device or media or voluntarily or involuntarily separates from the HCC, the HCC manager or designee shall obtain the devices and/or media and shall ask the Workforce Member to certify that he/she has not retained any PHI or made or kept copies of PHI. This should be done as part of the check-out process using the Property Clearance or Termination Checklist (available from the Office of Human Resources and on the HIPAA website); in cases of separation, or via written statement in other cases; and

   b. When a University-owned, University-leased, or personally-owned device that contains PHI is no longer needed for University Business or will be reused for a different purpose, the User shall contact his Tier 1 or IT Representative to ensure all PHI is completely removed with erase tools that meet industry standards for data destruction.

2. Disposal/Retirement Procedures – Each HCC must implement procedures to address the final disposition of PHI hardware or electronic media on which PHI is stored. At a minimum, each HCC's disposal/retirement procedure must make the PHI unusable, unreadable, or indecipherable. If the HCC uses an outside service provider for disposal or retirement services, the HCC manager or administrator must confirm with Purchasing that a Business Associate Agreement is in place with the service provider prior to using the vendor's services. HCCs should contact their Tier 1s or IT Representatives for assistance.

   a. All equipment awaiting pick-up for destruction or retirement must be kept in a secure area.

   b. Each Health Care Component, in coordination with its Tier 1 or IT Representative as appropriate, shall log the disposal or retirement of devices and electronic media on its inventory. At a minimum, the log must include the following information:
      i. Date and time of disposal or retirement

ii. Who performed the disposal or retired the device
iii. Brief description of media or information systems disposed of or retired
iv. Reason for disposal/retirement
v. Documentation of PHI removal or destruction prior to disposal/retirement (see *Record of Destruction* form on OUHSC IT web page for example). This documentation must be maintained by the HCC or its Tier 1/IT Representative for at least 6 years

C. Movement from Permanent Location - Each HCC must create or ensure it has a retrievable, exact copy of PHI, when needed, before moving devices or media that contain PHI from their permanent location. At a minimum, the procedure must:
   1. Identify and document the person, persons, or role that will create the data backup, such as the manager, Tier 1, or IT Representative.
   2. Require testing and validation of the success of the data backup prior to movement or major system change. (If the HCC uses Information Technology to create the back-up, the HCC's procedure may state that the HCC relies on Information Technology for testing and validation.)

HCCs should contact their Tier 1 or IT Representative for assistance with the above requirements.

IV. REFERENCES

1. HIPAA Regulations, 45 CFR 310(d)(2)
2. Applicable Information Technology policies

Type Of Device	Is Device Owned By The Employee? Owned By The University? Leased By The University? Other?	If Owned Or Leased By OU, Who Has Device Been Issued To? If Personally Owned, Name Of Owner?	Location Where Device Is Assigned Or Primarily Used.	Device Description (Manufacturer And Model), If Available	Serial Number Or Asset Tag, If Available	Use/Purpose	Encrypted	Type Of Encryption	Date Device Was Encrypted, If Known	Disposition Description And Date	Person Completing Entry	Additional Comments
Examples Include: Flash Drive, Laptop, Tablet, Phone, Portable Hard Drive, Desktop.	Ex: Personally Owned, University Owned, University-Leased	Ex: Dr. J Smith, Jan White	Ex: Neuro Clinic, Employee's Home, ORL Dept	Ex: Dell E6340 Laptop; MacBook Air 13; Sandisk Cruzer Edge 8GB	Ex: 123456789	Ex: Clinic Work, Patient Care, Research, Other University Business	Yes Or No (If No Include Date Scheduled For Encryption)	Secure Mobile; Mcafee End Point Encryption; Mcafee Native Encryption	Date	Ex: Active, Surplused, Returned To Vendor, Or Retired Through IT; Personal Device – Data Removed By IT. (Data Disposal Documentation Must Be Kept For All Devices Surplused.	Ex: J. Jones, Tier 1; S. Rowe, IT	Ex: Used For Notes

UNIVERSITY OF OKLAHOMA

HIPAA Policies

Title: Training – Privacy and Security	**Approved:** July 1, 2009
Effective Date: July 1, 2009	**Last Revised:** 4/1/2018

I. PURPOSE

To provide for training on University's HIPAA Policies and procedures.

II. POLICY*

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

On the Health Sciences Center campus, individuals who must take annual training are all volunteers, employees,** and University students/trainees. On the Norman campus, those individuals are all volunteers, employees, and University students/trainees in a designated Health Care Component. Individuals on both campuses who sign or are covered by a Business Associate agreement in their University capacity are also encouraged to take the annual HIPAA training (Note: The terms of the Business Associate agreement may also require such training.)

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

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

III. PROCEDURE

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

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

The training program, which may occur through or in conjunction with Information Security, shall also include periodic reminders and updates regarding HIPAA Security and may also include related IT Security policies, including but not limited to:

1. Guarding against, detecting, and reporting malicious software.
2. Monitoring log-in attempts and reporting discrepancies.
3. Creating, changing, and safeguarding passwords.

C. Tracking. It is the responsibility of each Health Care Component, in coordination with the Office of Compliance and/or Human Resources Office, to ensure that its employees, volunteers, and University students/trainees complete training according to the University's HIPAA Policies.

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

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

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

1. Regular Employees must complete the University's online HIPAA training within 5 days of becoming an employee. Health Care Component managers must also provide a written or oral review of their specific HIPAA Policies and procedures relevant to the employee's duties prior to giving the employees physical or electronic access to PHI.

2. Temporary Employees must complete the University's HIPAA training if they are expected to work for a Health Care Component for more than 5 consecutive days.** Training must be completed on or before the 6th day of providing services to the Health Care Component and may be completed online or on a printed version of the online course. Documentation of training must be maintained by the Health Care Component.

In addition, the Health Care Component manager must provide a review of its specific HIPAA procedures relevant to the temporary employee's duties prior to giving the temporary employee physical or electronic access to PHI.

a. Temporary Employees are required to execute the University's HIPAA *Terms of Access to PHI/ePHI* forms (available on the University's HIPAA website) prior to receiving access to PHI. The Health Care Component manager shall maintain that Agreement for at least six (6) years, or longer if required by other University policies

b. Temporary employees providing fewer than six consecutive days of services may be required by the Health Care Component to take the University's HIPAA training. The Health Care Component manager must, at a minimum, provide these individuals a

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

review of HIPAA Policies and procedures applicable to their duties prior to giving the temporary employee physical or electronic access to PHI.

3. Volunteers (excluding volunteer faculty) must complete the University's HIPAA training if they are expected to volunteer for a Health Care Component for more than 5 consecutive days.** Training must be completed on or before the 6th day of providing volunteer services and may be completed online or on a printed version of the online course. In addition, the Health Care Component manager must provide a review of its HIPAA policies and procedures applicable to the volunteer's duties prior to giving the volunteer employee physical or electronic access to PHI.

Volunteers (excluding faculty) must sign the applicable Terms of Access / Confidentiality and Security of Information Agreement (available on the University's HIPAA forms page) prior to receiving access to PHI. The Health Care Component shall maintain the Agreement for at least 6 years, or longer if required by other University policies.

Volunteers providing fewer than 6 consecutive days of volunteer services may be required by the Health Care Component manager to take the University's HIPAA training. The Health Care Component manager must, at a minimum, provide these volunteers a review of HIPAA Policies and procedures applicable to the volunteer's duties prior to giving the volunteer employee physical or electronic access to PHI.

4. Volunteer Faculty may be permitted to substitute annual HIPAA training received at another entity for the annual University HIPAA training if their Health Care Component verifies that the volunteer faculty member (a) does not have access to the University's network, and (b) does not provide the volunteer services at an OU facility or clinic, and (c) does not access OU patients or their PHI in their volunteer capacity. Volunteer faculty members must certify and document each year to the Health Care Component Training Coordinator that they have received annual HIPAA training elsewhere. The Health Care Component is responsible for maintaining these certifications and providing them to HIPAA Program Employees upon request. The Health Care Component may require the volunteer faculty to complete the University's annual HIPAA training if it prefers or if (a)-(c) cannot be verified.

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

6. Visiting Students/Trainees must either show proof of HIPAA training from their home institution (a copy of which must be maintained by their Health Care Component) or take the University's HIPAA training in accordance with D.3., whichever is required by the Health Care Component. Health Care Components supervising faculty must also provide a review, of its HIPAA policies and procedures applicable to the visiting students/trainees duties prior to giving the trainee physical or electronic access to PHI.

7. Others - Health Care Components must contact HIPAA Program Employees to determine the training requirements for any other individuals.

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

E. Material Changes. The University HIPAA Program Employees or Health Care Component manager shall provide training to those Workforce Members whose job or academic functions are affected by a material change in the University's HIPAA Policies within a reasonable period of time after the change becomes effective.

F. Sanctions**.** Employees who fail to complete the annual HIPAA training are subject to sanctions by the University of Health Care Component pursuant to HIPAA Sanctions policy. Colleges shall not permit students who fail to complete training to enroll for the next semester or session until training is complete. Temporary employees, visiting students/trainees, and volunteers (including volunteer faculty) who fail to complete annual training shall not be permitted by Health Care Components to provide services to or continue training at the University.

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

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

IV. REFERENCES

A. HIPAA Security Regulations, 45 CFR §164.308(a)(5)
B. HIPAA Privacy Regulations, 45 CFR §164.530(b)
C. HIPAA Sanctions policy
D. Terms of Access to PHI/ePHI forms – HIPAA forms page
E. Applicable Information Security policies

UNIVERSITY OF OKLAHOMA

HIPAA Policies

Title : Treatment, Payment, and Health Care Operations Uses and Disclosures	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Last Revised:** 4/1/2018

I. PURPOSE

To establish permitted Uses and Disclosures of Protected Health Information for Treatment, Payment, and Health Care Operations.

II. POLICY*

A. Health Care Components may Use or Disclose Protected Health Information for their own Treatment, Payment, or Health Care Operations as described in this policy.

B. Health Care Components may Disclose Protected Health Information:

1. for Treatment activities of another Health Care Provider;

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

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

   (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;

   (b) population-based activities relating to improving health or reducing health care costs;

   (c) protocol development,

   (d) case management and care coordination;

   (e) contact with Health Care Providers and patients with information about Treatment alternatives;

   (f) review of the competence or qualifications of Health Care Professionals;

   (g) evaluation of practitioner and provider performance;

   (h) 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;

   (i) non-health care professionals training; and

   (j) accreditation, certification, licensing, or credentialing activities.

C. Health Care Components that participate in an Organized Health Care arrangement may disclose Protected Health Information about an individual to another Covered Entity that participates in the Organized Health Care Arrangement for **any** Health Care Operations activities of the Organized Health Care Arrangement. Health Care Components should contact the Office of Legal Counsel or University Privacy Official for assistance in determining whether they are in an Organized Health Care arrangement.

D. For Uses and Disclosures of a patient's Protected Health Information other than for Treatment, Payment, and Health Care Operations of a Health Care Component or to another Health Care Provider, an Authorization from the patient must be obtained unless Disclosure pursuant to another policy is permitted and/or required. Health Care Components should review the HIPAA *Authorization to Use or Disclose PHI - Other Than to Patient* policy or contact the Office of Legal Counsel or the University Privacy Official for assistance.

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

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

See HIPAA *Mental Health Records, Substance Use Disorder Records, and Psychotherapy Notes* policy.

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

G**.** For Uses and Disclosures of PHI between Health Care Components and University departments that have not been designated as Health Care Components, an Authorization from the patient is required, unless the exchange is specifically permitted under the HIPAA Regulations.

H**.** Substance Use Disorder records maintained or created by a Health Care Component may be Disclosed only in accordance with 42 CFR Part 2, which requires consent beyond a general HIPAA Authorization. Health Care Components should contact the Office of Legal Counsel prior to releasing any Substance Use Disorder records. (See HIPAA *Definitions* policy and HIPAA *Mental Health Records, Substance Use Disorder Records, and Psychotherapy Notes* policy.)

III. REFERENCES

A. HIPAA Regulations, 45 C.F.R. 164.506, 42 CFR Part 2
B. FERPA, 20 USC 1232g; 34 C.F.R. Part 99

UNIVERSITY OF OKLAHOMA

HIPAA Policies

Title: Uses and Disclosures - Required and Permitted	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Last Revised:** 4/1/2018

I. PURPOSE

To outline general required and permitted Uses and Disclosures of Protected Health Information. (Policies governing specific Uses and Disclosures are included below.)

II. POLICY*

The University and University Personnel cannot Use or Disclose Protected Health Information, except as permitted or required by these HIPAA Policies and the HIPAA Regulations, summarized below.

A. Required Disclosures

The University and University Personnel are required to Use or Disclose Protected Health Information:

1. to a patient, when requested under, and as required by the HIPAA *Patient Access to Own Protected Health Information* policy; and the HIPAA *Accounting of Disclosures* policy; and
2. when required by the Secretary of the Department of Health and Human Services to investigate the University's compliance with the Privacy Regulations; and
3. as otherwise Required by Law (See HIPAA *Disclosures Required by Law* policy.)

B. Permitted Uses and Disclosures

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

1. For Treatment, Payment, or Health Care Operations, as permitted by and in compliance with the HIPAA *Treatment, Payment, and Health Care Operations Uses and Disclosures* policy;

2. Incident to a Use or Disclosure otherwise permitted or required by the HIPAA Regulations (such as to Business Associates or Personal Representatives), as long as the HIPAA *Minimum Necessary Rule* and HIPAA *Administrative and Physical Safeguards* policies are followed;

3. Pursuant to an Authorization as permitted by HIPAA *Authorization to Use or Disclose PHI* and HIPAA *Marketing* policies;

*Capitalized terms are defined in HIPAA *Definitions* policy

4. To family members and other involved in a patient's care, as permitted by, HIPAA *Disclosures to Family and Others Involved in Patient's Care* policy;

5. As permitted by and in compliance with HIPAA *Mental Health Records, Substance Use Disorder Records and Psychotherapy Notes*; *Disclosures Required by Law*; *Disclosures to Business Associates*; *Fundraising*; *PHI in Research*; and *Limited Data Set* policies;

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

7. By a Workforce Member who is the victim of a crime reporting to Law Enforcement, so long as the PHI disclosed is about the suspect and is limited name and address, date and place of birth, SSN, ABO blood type and rh factor, type of injury, date and time of Treatment, date and time of death if applicable, and distinguishing physical characteristics.

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

III. REFERENCES

A. HIPAA Regulations, 45 CFR § 164.502
B. HIPAA Regulations, 45 CFR § 164.512

UNIVERSITY OF OKLAHOMA

HIPAA Policies

Title: Verification of Identity	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Last Revised:** 4/1/2018

I. PURPOSE

To establish an identity verification process to be used prior to Disclosing PHI.

II. POLICY*

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

Verification of identity can be accomplished by: (1) review of picture I.D.; (2) signature comparison; or (3) other appropriate method. Determination of whether the individual is authorized to obtain PHI is still required. See HIPAA *Uses and Disclosures of PHI – Required and Permitted* and *Disclosures to Family and Others Involved in Patient's Care* policies.

B. This verification process is not required for Disclosures to family members or others involved in the patient's care, pursuant to HIPAA *Disclosures to Family and Others Involved in Patient's Care* policy.

III. PROCEDURE

A. To verify identity, University Personnel may rely on any of the following:

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

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

3. A request by an authorized Law Enforcement official who shows his/her badge or other official credentials if in person or uses the appropriate letterhead if the request is made in writing. Authority may be verified by written statement or legal process, warrant,

subpoena, order, or other legal process. (This goes to verification of identity of the official only; to determine whether the official is entitled to obtain the Protected Health Information, see HIPAA *Disclosures Required by Law* policy; and *Required and Permitted Uses and Disclosures* policy or contact the Office of Legal Counsel or the University Privacy Official.)

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

B. Any questions regarding verification of identity or an individual's authority should be directed to the supervisor, the Office of Legal Counsel, or the University Privacy Official. University Personnel should contact the Office of Legal Counsel or the University Privacy Official prior to responding to any written or verbal request by Law Enforcement Officials.

IV. REFERENCES

A. HIPAA Required and Permitted Uses and Disclosures policy
B. HIPAA Disclosures Required by Law policy
C. HIPAA Privacy Regulations 45 CFR §164.514 (h) (1)

UNIVERSITY OF OKLAHOMA

HIPAA Policies

Title: Waiver of HIPAA Rights Prohibited	**Approved:** October 8, 2002
Effective Date: April 1, 2003	**Last Revised:** 4/1/2018

I. PURPOSE

To prohibit a Health Care Component or Workforce Member from requiring patients to waive their HIPAA rights.

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 HIPAA Regulations as a condition of Treatment or Payment Activities.

III. PROCEDURE

A. Any Workforce Member who knows of a violation of this Policy shall promptly report the incident to the University Privacy Official, Office of Compliance, or a HIPAA Program Employee.

B. If the University Privacy Official, Office of Compliance, or a HIPAA Program Employee receives a report of a violation of this Policy, the University Privacy Official or designee will conduct an investigation to determine if a violation has occurred. If the report is substantiated, sanctions will be imposed pursuant to the HIPAA *Sanctions* policy.

IV. REFERENCES

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

UNIVERSITY OF OKLAHOMA

HIPAA Policies

Subject: Workstation Policy	**Approved:** January 2, 2014
Effective Date: January 2, 2014	**Last Revised:** 4/1/2018

I. PURPOSE

To ensure that computers that access, store, or transmit electronic Protected Health Information (ePHI) are used in a secure and appropriate manner.

II. POLICY*

Each Health Care Component and its Workforce Members who use computers that access, store, or transmit ePHI ("Users"), such as desktops, laptops, smart phones, flash drives, medical devices, and, tablets ("Workstations") must comply with the following policies.

A. Proper Use of Workstations
   1. Users shall observe the Minimum Necessary Rule at all times (i.e., use Workstations to Access only that PHI that they need to Access to perform a job-related function).
   2. Users shall not attempt to exceed their approved Access or attempt to Access any network, system, application, or data to which they have not been granted access.
   3. Users understand that Workstation use may be audited at the discretion of the HIPAA Security Officer, University Privacy Official, or University administration to confirm compliance with University policies.

B. Workstation Locations
   1. Users shall secure Workstations or shall locate them in areas that can be secured when they are not attended.
   2. Users shall position Workstation monitors away from view of those in common areas or install privacy screens to prevent unauthorized observation.
   3. Users must return the screens on Workstations to a password-protected screen saver or login screen when the Workstation will be unattended.

C. Storing PHI on Workstations
   1. Users shall not store ePHI on unencrypted Workstations.
   2. Users may store ePHI only on encrypted Workstations or on servers located in a secure enterprise data center.
   3. Each User is responsible for the security of his/her Workstation and the ePHI stored on the Workstation.
   4. Users must comply with all relevant IT Security and University policies concerning protecting ePHI stored on portable computing devices, such as password protection policies.

5. Portable computing devices used for University Business, regardless of whether the device is owned or leased by the University or by the User, must be encrypted.

NOTE: The Office for Civil Rights has stated that it considers storing ePHI on unencrypted portable devices to be an act of deliberate indifference with regard to the protection of PHI.

Users should Contact IT Security or the HIPAA Security Officer if they believe they have circumstances that warrant special encryption consideration.

D. Theft or Loss

1. Users must immediately report the theft or loss of any Workstation used for University Business (including those owned by the individual or a vendor) to the University Privacy Official and HIPAA Security Officer, as well as to their Tier 1/IT Representative or IT Security, so that mitigation and reporting options can be considered and implemented as soon as possible. (See HIPAA *Breach of Unsecured PHI/ePHI* policy.) It is expected that a police report will be filed with local law enforcement and that IT's *Lost/Stolen Device* form will be completed and submitted.
2. Users must cooperate with those individuals who are investigating the theft or loss of Workstations containing PHI and/or mitigating any related harm.

E. Updates and Security

1. Users shall cooperate with Tier 1s/IT Representatives to ensure Workstations are part of a patch or vulnerability management system that requires the application of regularly scheduled antivirus software updates.
2. Users shall comply with Information Technology password management policies and standards, such as those that require each User to have a unique User authentication.
3. Health Care Components and their Tier 1s/IT Representatives shall encrypt all portable computing devices before putting them into service.
4. Health Care Components shall require their Workforce Members to register their devices that connect to the Health Care Component or University network or other system containing PHI, as required by the Health Care Component's campus IT Security policy and other applicable policy.

5. Tier 1/IT Representatives shall maintain a current Device Inventory of all devices used to create, store, or maintain PHI, including but not limited to medical devices, desktops, laptops, tablets, smart phones, external storage and flash drives, in accordance with the HIPAA *Tracking, Returning, and Disposing of Device and Media* policies.

III. REFERENCES

A. HIPAA Regulations, 45 CFR 164.308(a)(1)(ii)(B)
B. HIPAA Regulations, 45 CFR 164.310
C. HIPAA Administrative and Physical Safeguards policy
D. HIPAA Breach of Unsecured PHI/ePHI policy
E. HIPAA Minimum Necessary Rule policy
F. Relevant Information Technology and IT Security policies