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