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

Access Control: the process of authorizing, establishing, modifying, and removing access to data and Information Systems.

Access Control Procedures: the functional steps taken to authorize and grant user accounts access to Information Systems and Information.

Access Rights: permission or privileges granted to an Information System (IS) or user to create, change, delete, or view data and files, as defined by rules established by IS Owners and the Information Security policy.

Account: see Student Accounts, Staff or Faculty Accounts, Sponsored Accounts, Admin Accounts, Shared Accounts, Service Accounts and/or Alumni Accounts.

Accountability: the ability to map a given activity or event to the responsible party to make the individual accountable for his/her actions.

Adverse Events: events with a negative consequence, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data.

Admin Accounts: Admin accounts will be created and maintained for staff with an Information Technology job description, including staff out of the Office of Information Technology and University Department Information Technology staff, that require extra privileges related to the management of a device or application. Admin accounts will be uniquely associated with a specific individual.

Alumni Accounts: Alumni accounts are accounts created for former students that have graduated or retired faculty or staff.

Asset: see Physical Asset and Software Asset.

Authentication: corroboration that a person is who he says he is.

Availability: the property that data or information is accessible and useable upon demand by an authorized person.
**Breach:** For HIPAA purposes, a Breach is the acquisition, access, use, or disclosure of protected health information (PHI) in a manner not permitted by law that compromises the security or privacy of the PHI.

**Business Associate:** a person or entity who is not a University 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 activities may include, but are not limited to, billing; repricing; claims processing and administration; data analysis; legal, accounting, and actuarial services; certain patient safety activities; consulting; benefits management; practice management; utilization review; quality assurance; and similar services or functions. A Business Associate may be a Covered Entity.

**Business Impact Analysis (BIA):** an OUHSC process that estimates the impact of losing the support of any Information System, establishes the escalation of that loss over time, identifies the minimum resources needed to recover, and prioritizes the recovery of processes and supporting system.

**Business Unit:** A Business Unit is:
1. One or more Workforce Members who are subject to the HIPAA regulations and who are engaged in providing a specific product or service that involves Protected Health Information on behalf of the University;
2. A part of the University which may effectively operate with some autonomy or, for the sake of analysis, be split out from the whole University for analysis and control purposes;
3. A group of cost centers that are performing similar administrative, educational, research, and/or healthcare services within a particular field of knowledge or area of specialization.

As applied to the University, a Business Unit may be a department, a program or school, a support service, or a central administration function within the University. A Business Unit may extend across multiple locations.

**Cardholder Data Environment (CDE):** area of computer system network that possesses cardholder data or sensitive authentication data and those systems and segments that directly attach or support cardholder processing, storage, or transmission.

**Category A – Healthcare Information Classification:** data that is legally regulated by the Health Insurance Portability and Accountability Act of 1996 to protect the confidentiality, integrity, and availability of the data. See *OU IT Data Classification Standard*.

**Category B – Payment Card Information Classification:** Data that is governed by Payment Card Industry (PCI) Data Security Standards to protect the confidentiality, integrity, and availability of the data. See *OU IT Data Classification Standard*.

**Category C – Student or Faculty Information Classification:** records that contain information directly related to a student and that are maintained by the University, and governed by the Family Educational Rights and Privacy Act (FERPA). See *OU IT Data Classification Standard*.

**Category D1 – Confidential Research and Publications Information Classification:** research data under which the University is obligated to protect the confidentiality and disclosure of data would impact the University’s mission to conduct research. See *OU IT Data Classification Standard*. 
**Category D2 – Research and Publications Information Classification:** research data generally available to the public, or is not under contractual or regulated obligations for data protection. See *OU IT Data Classification Standard.*

**Category E – University Administrative and Financial Information:** confidential University information requiring security and privacy protection. See *OU IT Data Classification Standard.*

**Category F – Public Information Classification:** Data that the University is under obligation to make available to the public. Data for which there is no expectation of privacy or confidentiality. Data that the University or its employees have the right to make and have chosen to make available or to publish for the explicit use of the general public.

**Classification:** the process of categorizing Information Systems and Data into distinct classes for the purpose of identifying Information Security control requirements.

**Clearing:** a level of media sanitization that would protect the confidentiality of information against a robust keyboard attack. Clearing does not allow information to be retrieved by data, disk, or file recovery utilities.

**Cloud Service Provider:** a company that offers some component of cloud computing – typically Infrastructure as a Service (IaaS), Software as a Service (SaaS), or Platform as a Service (PaaS) -- to other businesses or individuals.

**Computers:** are defined as all computer variations (desktop, laptop, notebook, etc.) owned by the University of Oklahoma that run a complete desktop operating system and are used for performance of job functions and/or business/instructional purposes.

**Confidentiality:** the property that data or information is not made available or disclosed to unauthorized persons or processes.

**Control:** a safeguard or countermeasure. Any administrative, management, technical, or legal method that is used to manage risk related to the confidentiality, integrity, and availability of data and Information System(s). Controls include practices, policies, procedures, programs, techniques, guidelines, organizational structures, and the like.

**Controlled Unclassified Information (CUI):** The University of Oklahoma, through its research mission, is subject to laws, regulations and government wide policies that require certain types of information to be safeguarded. Some of the labels or legacy markings used to describe information subject to these laws, regulations and policies include, but are not limited to:

- For Official Use Only (FOUO)
- Controlled Unclassified Information (CUI)
- Sensitive But Unclassified (SBU)
- Limited Official Use (LOU)
- Sensitive Unclassified Information (SUI)
- Law Enforcement Sensitive
- DEA Sensitive
- Official Use Only (OUO)
- Department Of Defense (DoD) Technical Information
- Distribution Statements on Technical Documents
- Sensitive Security Information
- Protected Critical Infrastructure Information
- Unclassified Controlled Nuclear Information
- Export-Controlled Information

**Covered Entity:** the entities to which the Privacy Regulations apply, including the University because it is a Health Plan and/or a Health Care Provider that transmits any Health Information in electronic form in connection with 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.

**Cybersecurity Incident:** A violation or Imminent Threat of violation of computer security policies, standard security practices, confidentiality, integrity, availability, possession or control, authenticity, utility, or safety of information systems. It also means the loss of data through theft or device misplacement or loss, all of which may have the potential to put the data at risk of unauthorized access, use, disclosure, modification, or destruction. A Cybersecurity Incident that compromises the privacy of PHI or PII is treated as a possible HIPAA breach.

Note: This definition excludes incidents that are not security related such as natural disasters and power failures.

**Data Aggregation:** any process in which information is gathered and expressed in a summary form, for purposes such as statistical analysis.

**Data Manager:** appointed for each project that creates and/or uses institutional data. A Data Manager is responsible for ensuring their project implements and enforces data governance policies, a responsibility that applies during the entire life cycle of the project. This includes infrastructure security, data access policies, and creation and maintenance of any project-specific data definitions and/or appropriate use guidelines.

**Data Owner:** a senior university administrator accountable for the creation and maintenance of one or more authoritative sources of data relied upon for key university operations. Data Owners have authority over and are responsible for strategic planning and setting policy. Data Owners appoint Data Steward(s) over specific subject area domains.

**Data Steward:** appointed by an Information System or Data Owner to develop and implement rules and procedures needed to ensure data and security policies set by the Data Owner are enforced. An Information System or Data Steward is typically a high-level functional end user within an operational area who is deemed an expert in using data managed by that area. S/he is responsible for ensuring data quality and integrity, authorizing access, monitoring appropriate use, and providing documentation and training to support institutional data needs.

**Data User:** any person using institutional data. This includes faculty, staff, students, and contractors. Access to institutional data is contingent on following all applicable policies and procedures and can be revoked in cases of inappropriate use.

**Degaussing:** erasing information from a magnetic disk, tape, or other magnetic storage device.
**Destroying**: a form of sanitization that ensures media cannot be reused as originally intended, after destruction.

**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.

**DFARS**: Defense Federal Acquisition Regulation Supplement, a Department of Defense-specific supplement to the FAR (Federal Acquisition Requisition). It provides acquisition regulations that are specific to the DoD. DoD government acquisition officials and contractors doing business with the DoD must adhere to the regulations in the DFARS.

**Disaster**: an unplanned event resulting in significant damage, destruction or extended loss of IT services provided to the University, including: a) an interruption to Essential IT Services (core network, voice service, central computing facilities, enterprise applications), b) workforce disruption. Interruptions can include the loss of third-party infrastructures that are not the property of OU IT, but critical to IT operations (e.g., power grids, telephone switching centers, or OneNet).

**Disclosure**: the release, transfer, provision of access to, or divulging in any other manner of information outside of the University.

**Disposal**: the act of discarding media with no other sanitization considerations. This is most often done by recycling paper containing non-confidential information but may also include hardware and/or electronic media on which non-confidential data was stored.

**Electronic Protected Health Information (ePHI)**: individually identifiable health information stored, processed, transmitted, or received in electronic form or media.

**Electronic Media**: any device capable of storing electronic information. This includes memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card. This includes but is not limited to:

- Servers
- Workstations
- Portable Computing Devices
- Personal Digital Assistant devices
- Cell phones
- Magnetic storage media
- Floppy disks
- Compact disks
- Tapes
- Flash/Memory drives

**Electronic Personnel Action Form (ePAF)**: an electronic request form authorizing the creation,
modification, or termination of a staff, faculty, or student account.

**Emergency:** a sudden or unexpected occurrence or combination of occurrences that may cause injury, loss of life, or destruction of property or may cause the interference, loss, or disruption of a Business Unit’s normal operations to such an extent that it poses a threat to the campus community.

**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 for purposes of regulatory compliance.

**End User Device** include but are not limited to laptops, notebook computers, tablets, smart phones (iPhones/Android/Windows), desktop computers, connecting to the OU Network.

**Events:** are any observable occurrences in a system or network. Events include a user connecting to a file share, a server receiving a request for a web page, a user sending email, and a firewall blocking a connection attempt. Events can range from relatively harmless port scans to more serious attempts to penetrate the organization and occur almost constantly. In most cases, these occurrences do not require any action by the University and are dealt with by technical defenses already in place, such as anti-malware tools and intrusion prevention systems. Configuration and monitoring of these devices are relatively straightforward activities, conducted by either the IT Operations or the Security Operations organization.

**Externally derived research funds:** as it relates to computer purchases, refer to University accounts categorized as SPNSR, SP490, or NONSP (e.g., FAR/SRI distribution) funds within the PeopleSoft financial system.

**F**

**Facility:** the physical premises and the interior and exterior of buildings.

**Family Educational Rights and Privacy Act of 1974 (FERPA):** federal law that grants five specific rights to and governs disclosure of student electronic records of current and former students who have reached the age of 18 OR are attending a postsecondary institution.

**File Transfer Protocol with SSL Security (FTPS):** an extension to the File Transfer Protocol (FTP) that adds Secure Socket Layer (SSL)/Transport Layer Security (TLS)-based mechanisms/capabilities on a standard FTP connection.

**Funds:** see Externally derived research funds, Internally derived research funds, and University funds.

**G**

**Governance:** establishment of policies, and continuous monitoring of their proper implementation, by the members of a governing body of the University of Oklahoma.

**H**

**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.

**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 Officer, 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.)

---

**Incident Command System (ICS):** based on the National Incident Management System, ICS is an all-hazard, incident management concept. It allows users to adopt an integrated organizational structure to match the complexities, size, and demands of single or multiple incidents without being hindered by jurisdictional boundaries.

**Individual User:** see Data User.

**Essential IT Service:** an information system considered to be critical to the University and included in the University’s Continuity of Operations Plan. Essential IT Services have a maximum tolerable downtime of twenty-four hours or less.

**Mission-Critical IT Service:** an information system considered critical to a specific Mission,
College, Department, or Division with a maximum tolerable downtime of two days or less.

**IT Service:** an information system considered to be non-critical to the University and have a maximum tolerable downtime of three days or more. See also Essential IT Service and Mission-Critical IT Service.

**Information System:** including but not limited to University data, computer devices/equipment, software, operating systems, storage media, network resources and network accounts providing electronic mail, online browsing, and file transfer protocols.

**Imminent Threat:** a situation in which there is a factual basis for believing that a specific incident is about to occur; for example, when CERT issues a warning of an exploit that is rapidly spreading across the Internet and the University determines that its Information Systems are vulnerable to the exploit.

**Incident:** an occurrence on Information Systems – not necessarily malicious or requiring an action.

**Information System or Data Administrator:** an individual with principal responsibility for: the installation, configuration, security, and ongoing maintenance of an Information System (e.g., system administrator or network administrator). The Data Administrator role is performed by University Personnel with a named Information Technology job title.

**Institutional Data:** any data - structured or unstructured, detailed or aggregated - that are relevant to operations, planning, or management of any University unit. This includes (but is not limited to) any data that are reported to the OU Board of Regents; reported to federal and state organizations; generally referenced or required for use by more than one organizational unit; or are included in official administrative reporting.

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

**Internally derived research funds:** as it relates to computer purchases, refer to all other funds intended for research activities, including internally funded research grants, center, and startup funds.

**Internet of Things (IoT) Devices:** a system of connected smart devices, with the ability to transfer data over a network without requiring human interaction. IoT devices include, but are not limited to: gaming consoles, smart home assistants, smart appliances, wearable watches and trackers, streaming media devices, and wireless sensors.

**Internet Protocol (IP):** protocol by which data is sent from one Information System to another on the Internet.

---

**K**

**Kerberos:** a network authentication protocol designed to provide strong authentication for client/server applications by using secret-key cryptography.
Lightweight Directory Access Protocol (LDAP): a client/server protocol used to access and manage directory information.

Malicious Software: software such as a virus that is designed to damage or disrupt an Information System.

Maximum Tolerable Downtime (MTD): the maximum length of time an Information System can be inoperable without causing harm to the University.

Memoranda of Agreement/Understanding (MOA/MOU): a formal agreement between two or more parties to establish each party’s obligations or responsibilities.

Merchant: any entity that accepts payment cards bearing the logos of any of the five members of PCI SSC (American Express, Discover, JCB, MasterCard or Visa) as payment for goods and/or services. *Note – A merchant that accepts payment cards as payment for goods and/or services can also be a service provider, if the services sold results in storing, processing, or transmitting cardholder data on behalf of other merchants or service providers.

Minimum Necessary: see HIPAA Minimum Necessary Access Rule policy.

Non-Campus Location: refers to a location that is physically not part of the University of Oklahoma campus networks and that is not maintained by OU Health Sciences Center Information Technology personnel.

OUHSC: University of Oklahoma Health Sciences Center

OUMI: OU Medicine, Inc.

Password: a confidential Authentication composed of a string of characters.

Payment Card Industries (PCI) Data: data that include primary account number (PAN), full magnetic stripe data, CAV2/CVC2/CVV2/CID Codes, and PIN/PIN Block.

Peer-to-Peer (P2P): technology allowing individual users or “peers” to share files directly between desktop systems on the network without the need of a central server.

Permanent Location: approved locations for OUHSC staff, faculty, students, residents, affiliates, and volunteers to conduct University Business. Permanent locations may include OUHSC campus locations or approved remote access locations from OUHSC managed IS.

Personally Identifiable Information (PII): defined in state law regarding data breaches as an individual’s last name and first name or initial, with any of the following:
  • Social Security number
• Driver’s License number
• Date of Birth
• State ID card
• Passport number
• Financial account (checking, savings, brokerage, CD, etc.), credit card, or debit card numbers

**Physical Asset:** information technology devices including, but not limited to: desktop computers, laptop computers, smartphones, tablets, multi-function printer devices, medical devices, web servers, application servers, database servers, or network devices.

**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.

**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.

**PIN:** an identifying number allocated to an individual and used for validating electronic transactions.

**Policy:** the framework within which the University strives to meet its need for Information Security is codified as Security Policy. A Security Policy is a concise statement, by those responsible for a system (such as senior management), of information values, protection responsibilities, and organizational commitment.

**Procedures:** documented requirements for the ways certain tasks must be performed.

**Portable Computing and Storage Devices (PCD):** include but are not limited to laptops, notebook computers, tablets, smart phones (iPhones/Android/Windows), cell phones, thumb drives, alphanumeric pagers, memory cards, removable media, and external media such as Compact Disks (CDs) or DVDs.

**Preservation Hold:** also referred to as a legal hold, is a process that the University of Oklahoma uses to preserve forms of electronic information, potentially relevant when litigation is pending or reasonable anticipated.

**Q**

**R**

**Recovery Time Objective (RTO):** the time period after a disaster at which business functions need to be restored.
**Recovery Point Objective (RPO):** the time (relative to the disaster) to which data must be restored.

**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.

**Re-Use:** the use of electronic media for something other than its original purpose.

**Risk:** the likelihood that a specific threat will exploit certain vulnerability, and the resulting impact of that event.

**Risk Acceptance:** a decision where the cost of managing the risk without taking further steps is acceptable because the risk level is insufficient to justify the cost of mitigation.

**Risk Assessment:** the process of identifying, estimating, and prioritizing OUHSC Information Security risks resulting from the operation of an Information System.

**Risk Avoidance:** a decision to take steps to remove the risk or end the specific exposure.

**Risk Identification:** the process of identifying and examining exposures of an organization.

**Risk Management:** the program and supporting processes to manage Information Security risk to OUHSC that includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time. Risk can be managed in one of three (3) ways:
- Risk Mitigation
- Risk Acceptance
- Risk Avoidance
- Risk Transfer

**Risk Mitigation:** taking steps to reduce adverse effects of an identified risk.

**Risk Transfer:** transferring the risk to a non-University entity (e.g., cybersecurity insurance firm)

**Secure File Transfer Protocol (SFTP):** a secure version of File Transfer Protocol (FTP) that facilitates data access and data transfer over a Secure Shell (SSH) data stream.

**Secure Shell (SSH):** a cryptographic protocol and interface for executing network services, shell services, and secure network communication with a remote computer.

**Secure Socket Layer (SSL):** a standard protocol used for the secure transmission of documents over a network. SSL creates a secure link between a Web server and browser to ensure private and integral data transmission.

**Security Alert:** an indication of an event that is potentially actionable. A Security Alert can indicate a potential threat to confidentiality, integrity, availability, possession or control, authenticity, utility, or safety of Information Systems Security. Security Alerts may be received from event management sources or industry security groups and associations.
**Security Incident:** see Cybersecurity Incident.

**Security Measures:** all of the policies, procedures, standards, and controls that are in place to protect University information.

**Sensitive Data:** data in classification categories A or B of the OUHSC Information System and Data Classification Policy.

**Service Accounts:** Service accounts will be created and maintained for Information Systems to authenticate to other systems or applications without any association to an individual. Service accounts should be created sparingly and documentation of the purpose for them must be documented. The use of Service accounts must be periodically reviewed. Service accounts must not be used by people to authenticate aside from initial testing. Service accounts with elevated privileges must be closely monitored for abuse.

**Shared Accounts:** Shared accounts will be created and maintained only to support multiple users sharing the same identity. For example, these may be created when there is a need to share a set of resources or because a product implementation requires it. The use of Shared accounts is discouraged as it lacks accountability and the use of Shared accounts is prohibited for users accessing Category A, Category B, Category C, and Category D1 information.

**Simple Network Management Protocol (SNMP):** an Internet Standard protocol for collecting and organizing information about managed devices on networks and for modifying that information to change device behavior.

**Software Asset:** an application installed on a physical asset to process information.

**Sponsored Accounts:** Sponsored accounts will be created and maintained for other individuals (e.g., vendors, visiting faculty, collaborative research partners, contractors) who are authorized to be onsite, unescorted, and to use University Services and Facilities. Sponsored accounts will be uniquely associated with a specific individual.

**Standards:** specific requirements for the configurations of hosts and network security devices. These requirements tend to change slowly over time.

**Staff/Faculty Accounts:** Staff or Faculty accounts will be created and maintained for staff or faculty with a full- or part-time appointment and individuals with Emeriti status. Staff or Faculty accounts will be uniquely associated with a specific individual.

**Student Accounts:** Student accounts will be created and maintained for students admitted, enrolled, and attending the University or for students with an outstanding obligation to the University. Student accounts will be uniquely associated with a specific individual.

**Subject Matter Expert (SME):** an individual considered an expert in a specific subject.

**Surplus Equipment:** office equipment that is no longer needed for business activities. Surplus equipment must be disposed of or transferred in accordance with University policy.

**System Security Assessment:** an assessment conducted through interviews, documentation reviews, and testing of information security controls, by the System Security Governance, Risk, and Compliance team for Information Technology operated within the University of Oklahoma.
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.

Threat: an internal or external activity or event that has the potential to negatively impact the quality, efficiency, and profitability of the University of Oklahoma. Threats may be internal or external, natural or manmade, intentional or accidental.

Trainee: students and post docs, residents, fellows, and others who are not regular employees and whose primary focus at the University is education- or training-centered.

Transport Layer Security (TLS): a protocol that provides communication security between client/server applications that communicate with each other over the Internet. It enables privacy, integrity, and protection for data in motion.

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

University Business: Refers to employment-based responsibilities and academic responsibilities performed on behalf of or through the University by faculty, staff, volunteers, trainees, and other persons whose conduct, in the performance of work or responsibilities for or through 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 other portable device use, University Business includes, but is not limited to, the use of a laptop or device to access University email (including through webmail) and to access non-public University systems, networks, or data in the performance of work for the University.

University Funds: as it relates to computer purchases, refer to all University accounts and funding sources within PeopleSoft financial system that are NOT defined as internally or externally derived research funds.

University Personnel: see Workforce Member.

Use: the sharing, employment, application, utilization, examination, or analysis of University information.

User: see Data User.

Virtual Private Network (VPN): an encrypted tunnel from the OUHSC network through an Internet Service Provider (ISP) network to a remote location. VPN technology virtually extends the campus network to an off-campus location, such as an employee’s home.

Vulnerability: a weakness that if exposed to a threat, may result in harm and, ultimately, some form of loss.
**Workforce Members:** faculty, staff, volunteers, trainees, and other persons whose conduct, in the performance of work or assignments for or through the University or for or through its Business Associates, is under the direct control of the University or of its Business Associates, whether or not they are paid by the University or by its Business Associates (also referred to as University Personnel). 45 C.F.R. § 160.103.

**Workspace:** the space used or required for University Personnel functions at the University of Oklahoma.

**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.