Information Security Policy Definitions

Current Version	Compliance Date	Approved Date
3.2	03/31/2018	01/04/2019

A.

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 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.

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.

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.

B.

***Breach*:** accidental or intentional disclosure of Category A or Category B OUHSC data. *See Information System and Data Classification Policy.* 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.

C.

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 Classification: data and associated Information Systems that are legally regulated with a requirement to self-report to the government and/or provide notice to the individual if information is inappropriately accessed, such as:

- HIPAA data (PHI)
- Payment Card Industries (PCI)
- Personally Identifiable Information (PII)
- FERPA data

Category B Classification:

Data and associated Information Systems used in the conduct of University business, in which the data is not legally regulated, but for which an expectation of privacy or confidentiality exists;

Data that the Information System Owner and/or University executive leadership have determined not to publish or make public;

Data protected by contractual obligations;

All public-facing Information Systems (exposed to the Internet).

Category C Classification: data and associated Information Systems not generally available to the public and not regulated or under contractual obligations for data protection.

Category D 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 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.

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.

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,

Critical: functions or services offered that could not be interrupted or unavailable for several business days without significantly jeopardizing the University's ability to serve its students and the communities of Oklahoma.

***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.

D.

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

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.

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.

E.

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

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.

***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.

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.

G.

Guidelines: recommended practices for Information System security configurations. The failure to follow a guideline may indicate an area of concern but does not necessarily create vulnerability.

H.

Health Care Component(s): a component or combination of components designated by the University, a Hybrid Entity. The "Health Care Components" of the University of Oklahoma include the parts of the following areas that provide Covered Functions: (i) College of Medicine – Oklahoma City, including OU Physicians; (ii) School of Community Medicine (formerly College of Medicine – Tulsa), including OU Physicians-Tulsa; (iii) College of Pharmacy; (iv) College of Dentistry; (v) College of Nursing; (vi) College of Allied Health; (vii) College of Public Health; (viii) Development Office; (ix) Goddard Health Center; (x) the Athletics Department Center for Athletic Medicine and Psychological Resources for OU Student-Athletes; (xi) Information Technology; (xii) Internal Auditing; (xiii) the Office of Legal Counsel; (xiv) Counseling Psychology Clinic; (xv) HSC Financial Services; (xvi) NC Financial Support Services; (xvii) Office of Compliance; (xviii) Human Research Participant Protection Program/Institutional Review Board, and (xv) OUHSC Student Counseling Services.

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

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

Hybrid Entity: A single legal entity under HIPAA: (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). The University is a Hybrid Entity.

Hypertext Transfer Protocol Secure (HTTPS): a variant of the standard web transfer protocol (HTTP) that adds a layer of security on the data in motion through a Secure Socket Layer (SSL) or Transport Layer Security (TLS) protocol connection.

I.

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.

Information System: an interconnected set of information resources under the same direct management control that shares common functionality. An Information System normally includes hardware, software, information, data, applications, communications, and/or people.

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.

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

IS Administrator: An individual with principal responsibility for the installation, configuration, security, and ongoing maintenance of an IS (e.g., system administrator or network administrator). At OUHSC, the IS Administrator role is typically performed by the Business Unit Tier One. The IS Administrator role may be performed through a service level agreement between the Business Unit and OUHSC IT.

IS Owner: The individual responsible for maintaining a current inventory of all IS within the Business Unit, classifying the data and IS, establishing rules for disclosing and authorizing access to IS data, conducting access control reviews, coordinating with OUHSC IT to conduct risk assessments, and serving as the escalation contact for the IS Administrator.

IS Owner Representative: an individual designated by the IS Owner to act on his/her behalf.

IS Sponsor: An individual responsible for providing the necessary funding and support for the IS Owner and Administrator to perform their roles and responsibilities. The IS Sponsor provides executive oversight of data and/or IS and assumes responsibility for policy compliance for the IS under his or her control. The IS Sponsor reviews high level risk items of the IS and makes risk management decisions for the Business Unit.

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

J.

K.

L.

Lightweight Directory Access Protocol (LDAP): a client/server protocol used to access and manage directory information.

M.

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

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: standard under HIPAA that requires University personnel to make reasonable efforts to limit the use, disclosure of, and requests for protected health information to the minimum necessary to accomplish the intended purpose of use, disclosure or request. HITECH limits covered entities' discretion for determining what constitutes the minimum necessary and requires covered entities to initially limit the use, disclosure or request of PHI, to the extent practicable, to a limited data set or, if needed, to the minimum necessary to accomplish the intended purpose of such use, disclosure, or request. HITECH clarifies that the entity disclosing the PHI (as opposed to the requestor) is responsible for making the minimum necessary determination.

N.

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

O.

OUHSC: University of Oklahoma Health Sciences Center

OUMI: OU Medicine, Inc.

P.

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

Protected Health Information (PHI): individually identifiable health information that is transmitted by, or maintained in, electronic media or any other form or medium. See also, ***ePHI***.

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

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

Q.

R.

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

S.

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.

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

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

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.

T.

***Threat*:** the potential source of an adverse event.

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.

U.

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

V.

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.

W.

Workforce Members: 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.

X.

Y.

Z.

Revision History

Version	Date	Updates Made By	Updates Made
1.0	11/15/05	OUHSC IT Security	Baseline Version
2.0	11/18/2014	OUHSC IT Security	Updated Definitions
3.0	01/03/2018	OUHSC IT Security	Added: Access, Access Control, Adverse Events, Authentication, Breach, Classification, CSP, Cybersecurity Incident, Data Aggregation, Disclosure, Encryption, Events, Facility, FERPA, FTPS, HIPAA, HITECH, Hybrid Entity, HTTPS, ICS, Incident, IS Administrator, IS Owner, IS Owner Representative, IS Sponsor, IP, LDAP, Malicious Software, MOA/MOU, Password, Permanent Location, PIN, Risk Acceptance, Risk Avoidance, Risk Mitigation, SFTP, SSH, SSL, Security Alert, Threat, Use, TLS Removed: Control Review, Data Custodian, Data Owner, Electronic Storage Media, Enterprise Applications, Erase Tool, Local Support Provider, Purging, Product Review, Resource Owner, Resource Owner Representative
3.1	02/20/2018	OUHSC IT Security	Added: Merchant
3.2	10/26/2018	OUHSC IT Security	Updated PCD definition to include alphanumeric pagers.

Approval History

Version	Date	Approved By
3.1	03/06/2018	Information Security Review Board
3.2	01/04/2019	Information Security Review Board

Review History

Date	Reviewed By
01/03/2018	OUHSC Legal Counsel
01/24/2018	OUHSC Information Security Team

03/06/2018	OUHSC Information Security Review Board