UNIVERSITY OF OKLAHOMA HEALTH
Information Technology
Security Policies

Subject: Information Security Policy Definitions	**Coverage:** Health Care Components
Policy #: Information Security P# TBD	**Draft Date:** 11/15/05
Regulation: HIPAA**,** FERPA, GLB, OSF	**Approved:** 11/16/05
Effective: 11/16/05	**Revised:** 11/18/14

A ***Access rights:*** permission or privileges granted to users, programs or workstations to create, change, delete or view data and files within a system, as defined by rules established by data 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

Availability: the property that data or information is accessible and useable upon demand by an authorized person

B ***Business Associate*****:** a person or entity who

(1) on behalf of a University *Health Care Component* performs or assists in a function or activity involving the Use or Disclosure of Individually Identifiable Health Information, including claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; practice management; repricing; and other functions and activities; or
(2) provides legal, actuarial, accounting, consulting, Data Aggregation, management, administrative, accreditation or financial services that involves the disclosure of Individually Identifiable Health Information.

Business impact analysis (BIA): an exercise that determines the impact of losing the support of any resource to an organization, establishes the escalation of that loss over time, identifies the minimum resources needed to recover, and prioritizes the recover of processes and supporting system

Business unit**:**

(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 Covered Entity. (As applied to the University, a business unit may be a department, a program or school, a support service or central administration function within the University. A business unit may extend across multiple locations.)
(2) a part of the University which may effectively operate with some autonomy or for the sake of analysis it may be split out from the 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;

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 Data Classification: (highest level, most sensitive; restricted and vital) information of which loss, corruption or unauthorized disclosure, would seriously and adversely impact the academic, healthcare, research, or business functions of University. The impacts on University

could include any violation of privacy, security, financial, legal, research, business, or other contracts, or a violation of federal or state laws/regulations. Examples include, but are not limited to, statutorily protected medical information, patient medical charts, and litigation documents

More Specific Examples of Category-A Data

HIPAA - Protected Health Information

- Patient Names
- Street address, city, county, zip code
- Dates (except year) for dates related to an individual
- Telephone/Fax numbers
- E-mail, URLs, & IP numbers
- Social security numbers
- Account/Medical records numbers
- Health plan beneficiary numbers
- Certificate/license numbers
- Vehicle id's & serial numbers
- Device id's & serial numbers
- Biometric identifiers
- Full face images
- Any other unique identifying number, characteristic, or code
- Payment Guarantor's information

For more information, see the OUHSC HIPAA web page.

PCI DSS – Credit Card Data

- Primary Account Number (PAN)
- Full magnetic stripe data (cannot be stored)
- CAV2/CVC2/CVV2/CID Codes (cannot be stored)
- PIN/PIN Block (cannot be stored)

FERPA and GLB - Student Records and Financial Data

- Social Security Numbers (or numbers derived from them)
- Grades
- Student Financial Numbers (Bursar's office)
- Credit Card Numbers
- Bank Account Numbers
- Wire Transfers
- Payment History
- Financial Aid / Grants
- Student Bills
- Driver's License
- State ID

For more information, see OU FERPA web page.

Donor Information

- Name
- Graduating Class & Degree(s)
- Credit Card Numbers

- Bank Account Numbers
- Social Security Numbers
- Amount/what Donated
- Telephone/Fax Numbers
- E-Mail, URLs
- Employment Information
- Family Information (spouse(s) / children / grandchildren)
- Medical History (alumni/family who have major medical procedures performed at OUHSC)

Faculty/Staff Housing

Essentially all the information a Loan Broker would have for Faculty/Staff.

- Name / Spouse Name
- Credit rating / History
- Income Levels and Sources, etc.

Research Information

- Funding / Sponsorship information
- Human subject information

General Information

- Office of the Legal Counsel Files

Employee Information

- Social Security Number
- Salary
- Name
- Date of Birth
- Home Address or Personal Contact Information
- Performance Reviews

Business Data

- Credit card information
- Contract information (between OU and a third party)

Access Control Data

- Passwords
- Personal Identification Numbers (PINs)
- Account names
- User-IDs

Category B Data Classification: (Moderate level of sensitivity; critical and vital) information of which loss, corruption or unauthorized disclosure would tend to impair the business or research functions of University, or result in potential business, financial, or legal loss. Examples include medical information (except that which is category A), appointment

schedules, department financial information, purchasing information, and University strategy documents.

Category C D*ata Classification:* (Very low, but still some sensitivity) information of which loss, corruption or unauthorized disclosure would result in minimal business, financial or legal loss BUT involves issues of convenience, ease of operation, personal credibility, reputation, or other issues of personal privacy. Examples include internal phone lists and private email addresses.

Category D D*ata Classification:* (not sensitive; unrestricted or public) information of which loss or exposure would have no impact. This information may be made generally available without specific information owner's designee or delegate approval. Examples include student directory information (See FERPA for a description), public phone directories, and campus maps.

Clearing**:** - Clearing information is a level of media sanitization that would protect the confidentiality of information against a robust keyboard attack. Simple deletion of items does not suffice for clearing. Clearing does not allow information to be retrieved by data, disk, or file recovery utilities. It must be resistant to keystroke recovery attempts executed from standard input devices and from data scavenging tools. One method to clear media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that is damaged or not writeable. The media type and size may also influence whether overwriting is a suitable sanitization method.

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

Control - Controls are safeguards or countermeasures. A Control is any administrative, management, technical, or legal method that is used to manage risk related to the confidentiality, integrity, and availability of data and IT resources. Controls include things like practices, policies, procedures, programs, techniques, technologies, guidelines, and organizational structures.

Control Review - A part of the risk management process which compares existing controls for data and/or information resources with respect to defined security requirements. A Control Review allows the resource to be analyzed by Information Technology and the Resource Owner to determine if the resource has the appropriate controls in place.

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

D ***Data Custodian:*** refers to those who conduct data processing services for the organization's software applications, data, networks, operating systems, etc.

Data Owner: refers to individuals responsible for data created, used, or stored in organizational computer systems.

Degaussing: is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes. Degaussing is not effective for purging nonmagnetic media, such as optical media [compact discs (CD), digital versatile discs (DVD), etc.).

Destroying: is the ultimate form of sanitization. After media is destroyed, it cannot be reused as originally intended. Physical destruction can be accomplished using a variety of methods, including disintegration, incineration, pulverizing, shredding, and melting. If destruction is decided upon due to the high security categorization of the information or due to environmental factors, any residual medium should be able to withstand a laboratory attack. *Disintegration, Incineration, Pulverization, and Melting* are designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. *Shredding* can be used to destroy flexible media such as diskettes once the media is physically removed from their outer containers. The shred size of the refuse should be small enough that there is reasonable assurance in proportion to the data confidentiality level that the information cannot be reconstructed. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, and CD-ROM), optical disks (DVD), and magneto-optic (MO) disks must be destroyed by pulverizing, crosscut shredding or burning. When material is disintegrated or shredded all residues must be reduced to nominal edge dimensions of five millimeters and surface area of twenty-five square millimeters. Destruction of media should be conducted only by trained and authorized personnel. Safety, hazmat, and special disposition needs should be identified and addressed prior to conducting any media destruction.

Disposal**:** Disposal is 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 maintained or transmitted in electronic form or media.

Electronic Media:

(1) Electronic storage media including 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; or

(2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission.

Electronic Storage 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
- Desktop Workstations

- Laptop Computers
- Personal Digital Assistant (PDA) devices
- Cell Phones
- Magnetic Storage Media
- Floppy Disks
- Hard Disks
- CDs
- Tapes
- Flash/Memory Drives

Emergency : a sudden or unexpected occurrence or combination of occurrences that may cause injury, loss of life, destruction of property or cause the interference, loss or disruption of a unit's normal business operations to such an extent that it poses a threat to the campus community. An emergency is something that may overwhelm the University's ability to resolve the situation

Enterprise Applications: include but are not limited to:

- PeopleSoft: Human Capital, Student Administration, Financials
- MS Exchange email
- IDX

Erase Tool: hardware or software that is capable of completely removing all recorded material from electronic media.

F

G ***Guidelines:*** recommended practices for host and network security device 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, which is a hybrid entity. The "health care components" of the University of Oklahoma include the: (i) College of Medicine – Oklahoma City, including OU Physicians; Graduate college (ii) the College of Medicine – Tulsa, including OU Physicians-Tulsa; (iii) College of Pharmacy; (iv) College of Dentistry; (v) College of Nursing; (vi) College of Allied Health; (vii) College of Public Health; (viii) Goddard Health Center; (ix) George Nigh Rehabilitation Institute; (x) the Athletic Department; (xi) Internal Auditing; (xii) the Office of Legal Counsel; (xiii) the General Clinical Research Center; (xiv) HSC Financial Services; (xv) NC Financial Support Services; (xvi) Office of Compliance; (xvii) Human Research Participant Protection Program/Institutional Review Board, and (xviii) OUHSC Student Counseling Services. For an up-to-date listing of HCC see http://www.ouhsc.edu/hipaa/docs/PrivacyPolicyManual.pdf definitions

I ***Imminent threat of violation***: refers to a situation in which there is a factual basis for believing that a specific incident is about to occur. For example, if CERT issues a warning of an exploit that is rapidly spreading across the Internet and the University determines that its systems are vulnerable to the exploit.

Information Security Incident:

(1) the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system;
(2) a security-related *adverse event* affecting the confidentiality, integrity, or availability of an information system or data;

(3) a violation or *imminent threat of violation* of information system policies, standards, or practices.

Examples include: hacking, password cracking, computer virus infection, denial of service attack, or violation of acceptable use of information systems.

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

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

Information system resource: an application or supporting infrastructure as determined by the resource identification process.

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

J

K

L ***Local Support Provider:*** An individual with principal responsibility for the installation, configuration, security, and ongoing maintenance of an information technology device or resource (e.g., system administrator or network administrator). When there is no formally identified local support provider (e.g., a personally owned computer used from home to connect to the University network) the user is the local support provider.

Tier ones support many departmental IT systems and desktop computers. Online Tier One directory

M ***Minimum Necessary:*** University Personnel must make reasonable efforts to limit the Use, Disclosure of, and requests for protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure or request.

Minimum Necessary (HITECH): 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 requester) is responsible for making the minimum necessary determination. The Secretary is required to issue guidance on what constitutes minimum necessary no later than August 17, 2010. At such time, this requirement to use a limited data set, or if needed, the minimum necessary to accomplish the intended purpose will go away and uses, disclosures, or requests will have to comply with the new minimum necessary guidance to be issued by the Secretary.

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

O **OUHSC:** Oklahoma University Health Sciences Center.

Organizational Security Policy: governance documents or statements concerning security that are formally defined and approved by an organization; security policies reflect the intent of the organization, but they are NOT configuration settings, detailed process definitions, detailed operational ***guidelines***, ***standards*** or ***procedures.***

P ***Peer-to-Peer (P2P) file sharing:*** technology allows individual users or "peers" to share files directly between desktop systems on the network without the need of a central server.

Personally Identifiable Data (PID): any name or number used in conjunction with any other information to identify a specific individual, including any (A) name, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number; (B) unique biometric data, such as (i) a fingerprint; (ii) a voice print; (iii) a retina or iris image; or (iv) any other unique physical representation; (C) unique electronic identification number, address, or routing code or (D) telecommunication identifying information or access device (as defined in section 1029(e) of title 18, United States Code)

Policy: the framework within which an organization 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. U.S. GAO. See ***organizational security policy.***

Procedures: procedures define requirements for the ways certain tasks must be performed. Some procedures, such as those for change management, define how changes occur on hosts and network security devices in response to business needs or evolving threats. Not following procedures may lead to host or network failures (e.g., when untested patches are installed and hosts fail), and can also lead to vulnerabilities that are introduced or not corrected (e.g., when an inappropriate rule is installed on a firewall or a vulnerability is not quickly patched).

Portable Computing Device (PCD): includes but is not limited to notebook computers; tablet PCs; handheld devices such as Portable Digital Assistants (PDAs), Palm Pilots, Microsoft Pocket PCs, RIM (Blackberry); smart phones; and converged devices.

Purging: is a media sanitization process that protects the confidentiality of information against a laboratory attack where clearing media would not suffice. A laboratory attack would involve a threat with the resources and knowledge to use nonstandard systems to conduct data recovery attempts on media outside their normal operating environment. This type of attack involves using signal processing equipment and specially trained personnel. Executing the firmware Secure Erase command for ATA drives and degaussing are examples of acceptable methods for purging. Degaussing of any hard drive assembly usually destroys the drive as the firmware that manages the device is also destroyed.

Product Review: part of the risk management program, it allows the resource owner to determine the risk level of the resource and identify the controls in place for the resource. It also allows the resource to be analyzed by Information Technology to determine if the resource has the appropriate controls, if it can function and be supported, and if it brings any additional or unacceptable risks to the infrastructure.

Q

R ***Resource Owner:*** refers to the individual responsible for an information resource. The resource owner may or may not be the data owner of the data associated with the resource. At OUHSC the resource owner must be a Department Budget Unit head or above.

Resource Owner Representative: An individual designated by the resource owner to act in their behalf.

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 Assessment/Analysis: The process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, and other organizations, resulting from the operation of an information system.

Risk Management: The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, and other organizations, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time.

An organization can manage risk in four ways:

- Risk acceptance
- Risk avoidance
- Risk limitation
- Risk transference

S ***Security Incident:*** see *Information Security Incident*

Security Measures: All of the Administrative, Physical, and Technical Safeguards in an Information System.

Sensitive Data: Any information, which through loss, unauthorized access, or modification could adversely affect any of the missions of the university or the privacy of individuals. Some sensitive data is protected by law or regulation, while other data is determined to be sensitive by virtue of its importance to the mission of the university. Examples of sensitive data include credit card numbers, Social Security numbers, medical information, financial records, employee data, etc. Data in classification categories A or B of the *OU Data Classification* chart are considered *sensitive.* See definition of *Category A and B Data Classification.*

Standards: specific requirements for the configurations of hosts and network security devices. These requirements tend to change slowly over time. Not following standards can lead to legal exposures or to vulnerabilities an attacker could exploit.

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 ***Teleworking:*** performing official duties at a non-campus location according to a pre-arranged agreement.

U

V **Virtual Private Network (VPN):** VPNs provide an encrypted tunnel from the University network through an Internet Service Provider (ISP) network to a remote location. VPNs are the primary security mechanism for protecting information in transit. VPN technology virtually extends the campus network to an off-campus location, such as an employee's home. An encrypted VPN protects information as it flows across the Internet. However, by itself, the VPN does not examine the type of traffic that is passed over the encrypted channel. Integration with other protection technologies, such as intrusion prevention systems, allows some products to identify malicious traffic before it can enter the organization's internal network.

W	***Workforce Member:*** employees, volunteers, and other persons whose conduct, in the performance of work for OU, is under the direct control of the University, whether or not they are paid by OU. This includes full and part time employees, affiliates, associates, students, volunteers, and staff from third party entities who provide service to OU.
X	
Y	
Z	