

Information System Data in Motion Policy

Current Version	Compliance Date	Approved Date
3.2	12/31/2017	03/06/2018

1. Purpose

This policy defines safeguards required to protect the confidentiality and integrity of OUHSC data in motion over public networks and during transport outside of the Permanent Location.

2. Policy

All OUHSC IS Owners, Sponsors, Administrators, and Service Suppliers must implement reasonable and appropriate measures to guard against unauthorized access to and protect the integrity and confidentiality of University data transmitted over public networks (Data in Motion) or transported outside the Permanent Location. It is the responsibility of OUHSC IS Owners, IS Sponsors, IS Administrators, and Technology Service Suppliers to understand the requirements of their roles in securing OUHSC Data in Motion.

ALL OUHSC IS OWNERS, IS SPONSORS, IS ADMINISTRATORS, AND TECHNOLOGY SERVICE SUPPLIERS MUST:

1. Classify OUHSC data in motion, for which they are responsible, in accordance with the IT *OUHSC Information System and Data Classification Policy*.
2. Acknowledge and abide by the transmission and transportation safeguards below.

Appropriate Transmission or Transportation of electronic Protected Health Information (ePHI)

Transmission of ePHI must be in accordance with University HIPAA policies governing PHI use and disclosure.

1. Transmission of ePHI through e-mail must comply with the IT *OUHSC Email Transmission and Use Policy*.
2. ePHI transmitted over the web must be transmitted over Secure Sockets Layer (SSL), using only strong security protocols, such as Transport Layer Security (TLS).
3. The minimum necessary standard (see HIPAA Minimum Necessary Rule policy) must be observed when transmitting ePHI. Email transmitted within the University should be sent as a limited data set when possible. ePHI may not be included in the subject line of any message.
4. Upon patient request, ePHI may be emailed to a patient, unencrypted, only in accordance with the HIPAA Safeguards policy and any clinic or department policy.
5. All email messages that contain ePHI must include a confidentiality statement similar to the following:

This email, including any attachments, contains information that may be confidential or privileged and is intended for use of the individual or entity named above. If you are not the intended recipient, be aware that any disclosure, copying, distribution, or use of the contents is prohibited. If you have received this email in error, please notify the sender immediately by a "reply to sender only" message and destroy all electronic and hard copies of the email and attachments.

6. Workforce Members are discouraged from sending ePHI via text messaging. Those who chose to send ePHI via text messaging (SMS protocol) must encrypt incoming and outgoing messages that they elect to store and must ensure they use a secure gateway (e.g., HTTPS) if they send messages over an

Internet gateway. Workforce Members are cautioned, however, that if the recipient does not have the same text message encryption protocol, the text may not be secure.

7. Workforce Members who perform part or all of their duties at another facility must comply with that facility's policy on data in motion.
8. ePHI file transmissions must first be documented in the Information System Security Baseline maintained by OUHSC IT Security, as part of the IT OUHSC *Information Security Risk Assessment*, and must be transmitted only via FTPS, SFTP, or HTTPS.
9. All Portable Storage Media that contain ePHI must be encrypted in accordance with OUHSC's *Portable Computing Device Security Policy*.
10. Transportation of Portable Storage Media containing ePHI from its assigned Permanent Location must include a Record of Transport that includes and is maintained by the IS Owner or IS Administrator for a minimum of six (6) years:
 - a. What was transported
 - b. Date/Time stamp of transportation
 - c. Final destination
 - d. Purpose for transportation
 - e. Who handled the ePHI during transportation
 - f. Date/time stamp of arrival
 - g. Condition of media
 - h. Frequency of transport

Portable Storage Media transporting ePHI must be clearly marked as "Confidential" during transport and must have a tracking number associated with it.

Appropriate Transmission or Transportation of Electronic Payment Card (PCI) Data

1. Transmission of Payment Card Data must be in accordance with OUHSC Payment Card Industries Data Security Standards. (See *Payment Card Industry Data Security Standard*.)
2. Transmission of Payment Card Data through e-mail is prohibited.
3. Payment Card Data transmitted over the web must be transmitted over Transport Layer Security (TLS).
4. Payment Card Data file transmissions must be transmitted only via FTPS, SFTP, or HTTPS.
5. All Portable Storage Media containing Card Holder Data must be labeled as "Category A" and "Restricted for Authorized Access Only."
6. Appropriate approval by the merchant account creator/owner must be obtained prior to transporting data.
7. All Portable Storage Media containing Payment Card Data that is being transported must be transported using a trackable courier or delivery method that provides transit tracking and confirmation of receipt.
8. All Portable Storage Media that contain Payment Card Data must be encrypted in accordance with OUHSC IT's *Portable Computing Device Security Policy*.
9. Transportation of Payment Card Data must include a Record of Transport that includes, and must be retained by the Merchant according to the Merchant's Records Retention standards:
 - a. What was transported
 - b. Date/Time stamp of transportation
 - c. Final destination
 - d. Purpose for transportation
 - e. Who handled the data during transportation
 - f. Date/time stamp of arrival
 - g. What was its condition
 - h. Frequency of transport
 - i. The tracking number associated with the xxx.

Appropriate Transmission or Transportation of Other Regulated (FERPA, GLBA, ITAR, Controlled Unclassified Information [CUI]) and Category B Data

1. Other regulated or Category B data transmitted over the web must be transmitted over Secure Sockets Layer (SSL), using only strong security protocols, such as Transport Layer Security (TLS).
2. All email messages that contain other regulated or Category B data must include a confidentiality statement similar to the following:

This email, including any attachments, contains information that may be confidential or privileged and is intended for use of the individual or entity named above. If you are not the intended recipient, be aware that any disclosure, copying, distribution, or use of the contents is prohibited. If you have received this email in error, please notify the sender immediately by a "reply to sender only" message and destroy all electronic and hard copies of the email and attachments.

3. Other regulated and Category B data file transmissions must first be documented in the Information System Security Baseline maintained by OUHSC IT Security, as part of the IT OUHSC *Information Security Risk Assessment*, and must be transmitted only via FTPS, SFTP, or HTTPS.
4. All Portable Storage Media that contain other regulated and Category B data must be encrypted in accordance with OUHSC's *Portable Computing Device Security Policy*.

3. Roles and Responsibilities

OUHSC Staff, Faculty, Students, Affiliates, Residents/Trainees, Volunteers, and Contracted Third Parties (e.g., Vendors, Business Associates) are responsible for the following:

- Understanding and complying with the OUHSC Security requirements when transmitting University data electronically.
- Transmitting electronic University data via acceptable methods only, as described in this policy.

4. Definitions

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

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.

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.

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 an customer support 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 Sponsor: An individual responsible for providing the necessary funding and support for the IS Owner and Administrator to perform their roles and responsibilities under this policy. 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 treatment decisions for the Business Unit.

Information System (IS): A system and/or service that typically includes hardware, data, applications, and communications that support an operational role or accomplish a specific objective. *Note – An IS can reside on or off University premises.

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 result in storing, processing, or transmitting cardholder data on behalf of other merchants or service providers.

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

Permanent Location: Designated primary locations for OUHSC staff, faculty, students, residents, affiliates, and volunteers to conduct University Business. Permanent locations may include OUHSC campus locations or remote access locations from OUHSC-managed IS. When referring to electronic devices, the Permanent Location is the primary location where the device is expected to be used or housed.

Portable Storage Media: Any portable 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, external hard drives, USB flash drives, or digital memory cards.

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.

Secure File Transfer Protocol (SFTP): A secure version of File Transfer Protocol (SFTP) 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.

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 the data in motion.

5. Enforcement

This policy is authorized and approved by the OUHSC Senior Vice President and Provost and enforced by the IT Chief Information Officer. Internal Audit and other authorized departments of the University may periodically assess Business Unit compliance with this policy and may report violations to the University Administration and Board of Regents.

6. Scope

This policy is applicable to all OUHSC faculty, staff, students, employees, Business Associates, contractors, vendors, OU Health Care Components, and others entrusted with University data.

7. Regulatory References

- State of Oklahoma Information Security Policy, Procedures and Guidelines 7.10 - Encryption
- HIPAA 45 CFR 164.312(e)(1)
- HIPAA 45 CFR 164.312(e)(2)(i), (ii)
- Payment Card Industries Payment Card Data Security Standards (PCI DSS)
- Gramm-Leach-Bliley Act Safeguards Rule

- U.S. Department of Education Privacy and Technical Assistance Center

8. Review Frequency

This policy is scheduled to be reviewed, updated, and modified annually, or more often as necessary.

9. Revision, Approval, and Review

Table 1 Revision History

Revision Date	Version	Revised By	Changes Made
04/11/2007	2.0	Ouhsc IT	Baseline Version
03/05/2017	2.1	Ouhsc IT	Updated Policy Statements to Define Explicit Responsibilities
03/15/2017	2.2	Ouhsc IT	Applied new Security Policy Template
04/03/2017	2.3	Ouhsc IT	Modified policy statement and transmission of email
11/15/2017	3.0	Ouhsc IT	Combined Transportation of Media policy and Transmission of Sensitive Data into one policy, "Data in Motion" policy. Modified transportation of Portable Storage Media policy statements. Added definitions.
11/27/17	3.1	Ouhsc IT	Modified Purpose Statement and made minor changes to PCI and Enforcement sections.
02/20/2018	3.2	Ouhsc IT	Updated policy statements and definitions.

Table 2 Approval History

Version	Approval Date	Approved by:
2.0	04/11/2007	Dean's Council
3.2	03/06/2018	Information Security Review Board (ISRB)

Table 3 Review History

Version	Review Date	Reviewed by:
2.0	11/20/2014	Ouhsc IT
2.1	03/05/2017	Ouhsc IT
2.2	03/15/2017	Ouhsc IT
3.0	11/15/2017	Ouhsc IT
3.1	11/27/2017	Ouhsc IT
3.1	01/23/2018	Legal Counsel