UNIVERSITY OF OKLAHOMA
Information Technology
Security Policies

Subject: Information System Transmission of Sensitive Data Policy	**Coverage:** OUHSC
Policy #: Information Security-P#10.8.1	**Version:** 2.0
Regulation: HIPAA, GLB, State of Oklahoma, PCI DSS	**Approved:** 04/11/07
Effective: 04/11/07	**Revised/Reviewed:** 11/20/2014

Policy Summary:	Information System Resource and Data Owners must appropriately protect sensitive data from unauthorized interception, modification, and access during electronic transmission.
Purpose:	This policy reflects our commitment to identify and implement security controls which will keep risks to information system resources at reasonable and appropriate levels.
Policy:	Information System Resource and Data Owners must establish controls to safeguard the confidentiality and integrity of sensitive data during transmission over an electronic communications network. Encryption must be used when required by law, regulatory requirement or University policy, and when determined necessary by the Data and Resource Owners. Encryption mechanisms must meet established industry and government standards. See Encryption Standards (FIPS).
Documentation:	All data collected and/or used as part of the Risk Management Process and related procedures will be formally documented and securely maintained.
Scope/Applicability:	This policy is applicable to all OUHSC Information System Resource and Data Owners.
Regulatory Reference:	HIPAA 45 CFR 164.308(a)(1)(ii)(B) 16 CFR Part 314 Standards for Safeguarding Customer Information [section 501(b) of the Gramm-Leach-Bliley Act (‘‘G–L–B Act’’) State of Oklahoma Information Security, Policy Procedures Guidelines. Payment Card Industry Data Security Standard (PCI DSS)
Definitions:	See the Information Security Policy Definitions document for definitions
Responsible Department:	Each OUHSC business unit that manages its own information systems is responsible for complying with this policy.
Enforcement/Audit:	The university’s Internal Auditing department is responsible for monitoring and enforcement of this policy.
Related Policies:	Risk Analysis, Data Classification, Resource Identification, Resource Classification
Renewal/Review:	This policy is to be reviewed and updated as needed by IT Information Security Services.