UNIVERSITY OF OKLAHOMA
Information Technology
Security Policies

Subject: Access to Sensitive Data Policy	**Coverage:** OUHSC
Policy #: Information Security-P#11.2	**Version:** 2.2
Regulation: HIPAA, GLB, PCI DSS, State of Oklahoma	**Approved:** 03/14/07
Effective: 03/14/07	**Revised/Reviewed:** 11/12/2014

Policy Summary:	Access to sensitive data requires prior authorization. Processes must be in place for the authorization, establishment, review, modification and removal of access to sensitive data.
Purpose:	To establish processes to protect the confidentiality, integrity and availability of sensitive data and provide accountability for that access.
Policy:	For all information system resources classified as sensitive, documented processes/procedures must be in place to verify: 1. levels of access have been defined 2. access to the data/resource is authorized 3. the level of access is regularly reviewed 4. access is modified or revoked as individuals' status or roles change 5. 5. access to sensitive data is logged
Documentation	Data Owners or a delegate must formally document and maintain the processes and related procedures for compliance with this policy.
Scope/Applicability:	This policy is applicable to all OUHSC workforce members. Each OUHSC business unit that manages access to information system resources is responsible for complying with this policy.
Regulatory Reference:	HIPAA 45CFR Parts 160, 162, and 164.308(a)(1)(ii)(B), PCI DSS v1.2 (Requirement 7, 8, and 10), 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
Definitions:	See the Information Security Policy Definitions document for definitions
Responsible Department:	IT Information Security Services will review and maintain this policy.
Enforcement/Audit:	This policy is enforced by the University's Office of Compliance. The Internal Auditing department of the University of Oklahoma is responsible for the auditing and reporting of compliance with this policy.
Related Policies:	Data Classification, Resource Identification and Classification, Risk Management.
Renewal/Review:	This policy is to be reviewed and updated as needed by IT Information Security Services.