UNIVERSITY OF OKLAHOMA
Information Technology
Security Policies

Subject: Information System Business Associate Contracts Policy	**Coverage:** OUHSC
Policy #: Information Security-P#10.2	**Version:** 2.0
Regulation: HIPAA, GLB, PCI DSS, State of Oklahoma	**Approved:** 09/10/03
Effective: 9/10/03	**Revised/Reviewed:** 11/13/2014

Policy Summary:	The University may permit a business associate to create, receive, maintain, or transmit Sensitive Data on the behalf of the University only if it obtains satisfactory assurances from the business associate that it will appropriately safeguard the information.
Purpose:	This policy reflects the University's commitment to identify and implement security controls which will keep risks to information system resources at reasonable and appropriate levels.
Policy:	When another entity is acting as a business associate of the University, the business associate must appropriately and reasonably protect the Sensitive Data that it creates, receives, maintains or transmits on behalf of the University. There must be a written agreement between the two parties that requires the business associate to appropriately and reasonably safeguard the sensitive information. When a written agreement is not feasible, the University must make a good faith attempt to obtain satisfactory assurances that the business associate will safeguard the University's sensitive data, as would be required by a business associate contract, and document the attempt and any reasons that these assurances cannot be obtained. The transmission of Sensitive Data by the University to a health care provider concerning anything related to or regarding the treatment of an individual does not require a business associate agreement. All business associate agreements must be in a format approved by University Legal Counsel. New contracts with existing business associates do not have to be obtained specifically for this purpose, if existing written contracts adequately address the applicable requirements or can be amended to do so
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 workforce members.
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.
Definitions:	See the Information Security Policy Definitions document for definitions
Enforcement/Audit:	The Internal Auditing department of the University of Oklahoma is responsible for the monitoring and enforcement with this policy.
Related Policies:	Risk Analysis, Data Classification, Resource Identification and

	Classification
Renewal/Review:	This policy is to be reviewed and updated as needed by IT Information Security Services.
Procedures:	Data or Resource Owners or a delegate must formally document and maintain the processes and related procedures for compliance with this policy.