UNIVERSITY OF OKLAHOMA

HIPAA Policies

Title: Purchasing or Leasing Equipment or Contracting for Services Involving PHI	**Approved:** June 15, 2016
Effective Date: June 15, 2016	**Last Revised:** 4/1/2018; 12/18/2018

I. PURPOSE

To ensure that equipment and services that HCCs use that involve the receipt, storage, or transmission of University PHI do not put University PHI or systems at an unacceptable level of risk for compromise~~.~~ and appropriately document the service provider's responsibilities.

II. POLICY*

~~A.~~A. External Vendors/Providers. Health Care Components that purchase or lease equipment or acquire technology or services that receive, store, or transmit PHI must comply with University Purchasing and IT Security R.I.S.K. Program policies, described below.

This Policy applies to but is not limited to purchases, leases, and contracts for services related to software, transmission services, network printers and copy machines, cloud storage, medical equipment and devices, computing devices, and technology services. This Policy applies regardless of the dollar amount of the transaction and regardless of how the transaction will be billed or paid.

Small dollar and P-card purchases are subject to this policy. Sole source purchases are subject to this policy.

1. Equipment/Software: Prior to purchasing or leasing the equipment or software described above, Health Care Component managers or administrators must contact IT Security and ask that a review of the product's security features and risks be completed. IT Security will evaluate the security features and issue recommendations regarding how to address or mitigate any risk identified, such as by implementing a technical control for the product (the R.I.S.K. Program). Health Care Components are expected to comply fully with Information Technology's recommendations prior to using the equipment or software or to obtain written administrative approval to do otherwise.

   Health Care Component managers or administrators must inform the Purchasing Department if the equipment/software will be used for PHI so Purchasing can obtain a Business Associate Agreement if appropriate.

   Health Care Component managers or administrators must also inform the Purchasing Department if leased equipment or software will be used for PHI, so that Purchasing can ensure the leasing agreement (or Request for Proposal or Bid, as appropriate) includes a requirement that the vendor destroy or wipe the hard drive in a manner that complies with

HIPAA when the lease term ends and the vendor takes possession of the leased equipment or that permits the University to do so.

2. Services: Prior to contracting for the services described above, Health Care Component managers or administrators must inform the Purchasing Department that the services will involve the University's PHI, so that Purchasing can include Business Associate terms in the agreement with the service provider.

   If the services include the service provider accessing or using University servers or IT systems, the Health Care Component manager or administrator also must request that IT Security review the proposed access and make a recommendations regarding how to address any risk identified, such as by implementing a technical control for the vendor's access to the server or system (the R.I.S.K. program). Health Care Component managers are expected to fully comply with Information Technology's recommendations or to obtain written administrative approval to do otherwise.

3. Managed Services. If the services acquired are managed services that may impact the University's PHI, such as maintenance or administration of servers, devices, equipment, or information or technology systems that store, process, transmit, or provide for the protection of the University's PHI -- regardless of who owns the system(s) involved -- the Health Care Component manager or administrator must request that IT Security review and make recommendations regarding the proposed access and the adequacy and specificity of the responsibilities assumed by the service provider (the R.I.S.K. program). Health Care Component managers are expected to fully comply with Information Technology's recommendations or to obtain written administrative approval to do otherwise.

   If the services include access to the University's electronic medical or billing record systems, the Health Care Component shall not permit such access until the vendor has completed the required HIPAA *Terms of Access to PHI/ePHI* forms (see the HIPAA Forms page).

   The Health Care Component manager or administrator must inform the Purchasing Department that the services will involve University PHI, so that Purchasing can include Business Associate terms in the agreement with the service provider.

B. Internal Vendor/Providers. If the equipment or services will be provided by an internal University department, such as Information Technology, IT Security, or Printing Services, the Health Care Component must have in place a written document that specifies who is providing what equipment and/or service, that PHI is involved and must be maintained in confidence, and what specific services and/or equipment is being provided. ~~Health Care Components may contact the Purchasing Department, IT Security, the University Privacy Official, or the HIPAA Security Officer if they have questions regarding these requirements.~~

C. Health Care Components may contact the Purchasing Department, IT Security, the University Privacy Official, or the HIPAA Security Officer if they have questions regarding these requirements.~~C~~

D. If equipment or services are acquired through a contract managed by another office, such as the Office of Research Administration or Office of Research Services, that office shall be responsible for the actions attributed to Purchasing above.

III. REFERENCES

A. 45 CFR 164.306
B. Board of Regents Policy, 4.11, Buying and Selling Goods and Services
C. Purchasing Department Small Dollar Policy
D. Information Security R.I.S.K. Program Policy