THE UNIVERSITY OF UTAH®

Title: Vendors and Business Services Agreements
Number: G4-004J
Responsible Office: Privacy Office (PO)
Last Revision: November 15, 2017
Owner: Director, PO. 801-581-2121

I. OVERVIEW

A. This document is meant to provide guidance for the implementation of the Information Security Policy – Section J: Vendors and Business Services Agreements.

II. GUIDELINES

A. General Guidance

1. A contract is typically required when a third party not affiliated with the University of Utah is allowed to use or disclose confidential information – or has the ability to access it by virtue of the relationship. For example, custodial staff or software support may not allow the individual access to confidential information directly, but they could be exposed to it.

2. A contract should be utilized when storing or transmitting sensitive and restricted information to Cloud services not provided by the University, such as those provided by Google (Google Apps), Microsoft's Cloud, and/or Amazon. If protected health information is involved, a Business Associate Agreement is required.

B. General Contractual Safeguards for Sensitive and Restricted Data: A contract or addendum must be obtained from the Office of General Counsel.

C. Contractual Safeguards for Payment Card Industry (PCI – Credit Card Information): Please contact the Payment Card Administration Team. Their contact information is available at: http://fbs.admin.utah.edu/payment_card/contact/

D. Contractual Safeguards for Protected Health Information

1. The University of Utah has adopted the following standard with regards to sharing of information with a vendor or business associate. A contract is required if any of the following criteria are met:

a) A company or person who is not a member of the University of Utah entity workforce AND who, on behalf of the entity, performs, or assists in the performance of, an activity or function involving the use or disclosure of protected health information. Examples include external transcriptionists, translators, or 3rd party copy services.

b) Any organization that provides data transmission of protected health information on behalf of The University of Utah entity subject to HIPAA and, as a result, requires access on a routine basis to such protected health information. Examples include:

(1) A Health Information Exchange Organization, Regional Health Information Organization, E-prescribing Gateway, or each vendor that contracts with a University of Utah entity subject to HIPAA to allow that entity to offer a personal health record to patients as part of its electronic health record.

c) If a third party will have indirect exposure to restricted information, either physically or electronically. Indirect exposure can come in the form of physical

transportation of restricted data, transport of restricted data across a network, or having the ability to access restricted data even if it is not expressly part of the service being provided (i.e., custodial services, IT resource maintenance, etc.).

2. Examples Include:
   a) A third party administrator that assists a health plan with claims processing.
   b) A CPA firm whose accounting services to a health care provider involve access to protected health information/restricted data.
   c) An attorney whose legal services to a health plan involve access to protected health information/restricted data.
   d) A consultant that performs utilization reviews for a hospital.
   e) A health care clearinghouse that translates a claim from a non-standard format into a standard transaction on behalf of a health care provider and forwards the processed transaction to a payer.
   f) An independent medical transcriptionist that provides transcription services to a physician.
   g) A pharmacy benefits manager that manages a health plan's pharmacist network.
   h) A courier or other person transporting PHI/restricted data in paper or electronic format.
   i) A third-party who is accessing, maintaining, or servicing IT resources.
3. This contract must come in the form of a Business Associate Agreement facilitated through the Privacy Office. Please contact the Privacy Office at 801-581-2121.