SECTION 8: SPECIAL COMMODITY PROCEDURES

SUBJECT: DATA SECURITY AGREEMENTS Procedure #8.21

POLICY: The University of Washington has a standard Data Security Agreement (DSA)[1] that vendors must sign if the vendor will have access to University or Confidential Data as part of fulfilling its contract with the University.[2] The DSA prohibits unauthorized access and use of data by a vendor.

PROCEDURE: The DSA is frequently used in Information Technology (IT) contracts, particularly when a vendor will be performing a service for the University, or where the vendor's IT product will store University of Washington data.

The DSA should be included whenever the vendor will have access to University of Washington data. This occurs in situations where a vendor is storing, hosting, transferring, analyzing or interpreting University data to provide the University with analytics or other information; where a vendor is designing an IT "solution" for the University that will access University of Washington data; or where a vendor will simply be encountering University of Washington data in connection with a deliverable that is not related to University data on a wide scale, as is common in consulting contracts.

The DSA protects "University" data and "Confidential" data.

> **University Data:** University Data is any and all data within the University's possession, custody, or control, and any and all data that the University has disclosed to the Vendor.
>
> **Confidential Data:** Confidential Data is University Data that is very sensitive in nature and typically subject to federal or state regulations; proprietary rights under patent, copyright, trademark, or trade secret law; or privileged against disclosure in a civil lawsuit.

The main purpose of the DSA is to protect the University of Washington's internal and confidential data. The secondary purpose of the DSA is to ensure that the vendor stores and protects University of Washington data in a way that is compliant with state and federal privacy laws.

If the data that the vendor will have access to as part of its contract with the University includes Protected Health Information (PHI), the vendor must also be required to sign the University's HIPAA Business Associate Agreement (BAA).[3] PHI is healthcare information created by a healthcare facility, provider or other healthcare entity that

[1] Available at: http://f2.washington.edu/fm/ps/supplier-information/terms-and-conditions

[2] See UW Terms and Conditions #13

[3] See Policy 8.22

relates to the patient’s healthcare, health, condition or payment and which can or could potentially be used to identify the patient. The BAA protects the University from breaches of PHI by a vendor, which can lead to loss of federal funding.

The DSA protects University and confidential data by prohibiting the vendor from disclosing University data; regulating how the vendor must store and safeguard University data; prohibiting unauthorized “surreptitious” code; requiring that certain information the vendor be provided to the University; and requiring oversight, data transfer and destruction and breach notification procedures.