

**Commonly Asked Questions in Negotiating  
Terms contained within the Business Associate Agreement**

**May I delete the reference to Washington law in Section 1?**

No. The HIPAA privacy regulations create a minimum standard for the protection of health information nation-wide. The regulations allow for the possibility that state law is more protective of a patient's privacy or provides a patient greater access to protected health information. In these instances, state law may actually govern the use or disclosure of health information, not the HIPAA regulations. Thus, it is important for business associates to understand that use or disclosure of protected health information on behalf of UW Medicine must conform to both state and federal requirements.

**May I expand the requirement in Section 3 for reporting of unauthorized use or disclosure beyond five working days?**

This is a business decision and may impact the cost of notification in case of a breach. The maximum time UW Medicine generally accepts is twenty days.

**May I expand the requirement in Section 5 for amending the designated record set beyond five days?**

This is ultimately business decision, however, it is important to consider state law requirements and to consult with UW Medicine Compliance, to discuss the operational implications. Upon request for amendment of a medical record (contained within the designated record set), state law provides that a health care provider must correct or amend its records within ten days of the request (RCW 70.02.100). If unusual circumstances exist, state law provides for a maximum of twenty-one days to respond. The HIPAA privacy regulations, in contrast, allow a health care provider sixty days to respond. This provision tends to be an area in which considerable energy in negotiation is expended. The most important question to address is whether, in reality, the business associate holds the original designated record set such that they will be impacted by a short deadline.

**Can the BAA be multi-entity for vendors providing services to more than one entity?**

Yes, the BAA may include any/all UW Medicine entities. The BAA must have signature lines for each entity included, be signed by an authorized person from each entity, and be maintained in accordance with entity-specific records retention rules..

**May I remove the requirement that the BA provide individuals with access to their PHI?**

No, the BA must make PHI available in accordance with HIPAA and state laws governing access of individuals to PHI. See *UW Medicine Privacy Policy: PP-23 Access of Individuals to Protected Health Information (PHI)/Designated Record Set*.

**May the BA provide PHI to a subcontractor?**

Yes, but the BA must enter into a contract that meets the requirements of a business associate agreement or other arrangement with the subcontractor(s) to ensure that the same restrictions and conditions including the implementation of reasonable and appropriate safeguards to protect the information that apply to the BA also apply to the subcontractor.

**Is a Business Associate Agreement required for a data storage contract?**

Yes, if an entity maintains PHI on behalf of the University of Washington or UW Medicine, it is a business associate even if the entity does not actually view the PHI.

**What if the Business Associate is a governmental entity?**

When the BA is a governmental entity, UW Medicine may enter a Memorandum of Understanding to document the BA's privacy, security, and electronic exchanges assurances. The Memorandum of Understanding must contain the required elements of a BA Agreement.

**What if there is a suspected or discovered violation of a Business Associate Agreement?**

If a violation(s) of the Business Associate Agreement is suspected or discovered, the department manager or other individual initiating a contract is required to report the violation to UW Medicine Compliance and request investigation.