Applicability: UW Medicine

Policy Title: Use & Disclosure of Protected Health Information by Business Associates

Policy Number: PP-12

Superseded Policy(ies) or Entity Policy: N/A

Date Established: January 31, 2003

Date Effective: July 1, 2014

Date Revised: January 22, 2007; November 18, 2009; June 14, 2011; May 30, 2012; May 6, 2013; August 2, 2013

Next Review Date: July 1, 2017

PURPOSE AND SCOPE
Business Associates¹ (BA) are contractors and businesses who are not members of the University of Washington or UW Medicine workforce and who are, or will be, performing a service or activity for on behalf of the University of Washington or UW Medicine involving the use or disclosure of protected health information (PHI). The purpose of this policy is to describe the requirements that the BA must agree to in order for them to create, receive, maintain or transmit UW Medicine PHI.

This policy is applicable to all UW Medicine entities.

POLICY PRINCIPLES/STATEMENT
Department managers or other individuals initiating a contract evaluate the other party to the contract to determine whether all three criteria that define a BA exist:

1. The outside entity or individual is not a member of the University of Washington or UW Medicine workforce;

2. The outside entity or individual will be, or is, performing a service or activity “for” or “on behalf of” the University of Washington or UW Medicine; and

3. The services or activities of the outside entity or individual include creating, receiving, maintaining or transmitting PHI. (Note: If an entity maintains PHI on behalf of the University of Washington or UW Medicine, the entity is a BA even if the entity does not actually view the PHI.)

¹ Examples of “Business Associates” include lawyers, auditors, consultants, third party administrators, healthcare clearinghouses, data processing firms, billing firms or other covered entities that are utilized by covered entities to perform their healthcare activities and functions.
If the contract for services or goods meets all three of the BA contract criteria, the department manager or other individuals initiating a contract works with purchasing to complete the Business Associate Agreement (BAA). Then, the buyer from purchasing attaches the BAA (see UW Medicine Business Associate Agreement, Attachment A) to the contract and documents the BA in the Business Associate Inventory.

If the contract or purchase order is from another government agency, then a Memorandum of Understanding should be executed. The department manager or other individuals initiating a contract works with UW Medicine Compliance and Purchasing to complete a Business Associate Memorandum of Understanding and the buyer from purchasing attaches the memorandum to the contract/purchase order and documents the BA in the Business Associate Inventory.

**DEFINITIONS**

1. **Business Associate** means a person or entity, other than a member of the UW workforce, who creates, receives, maintains, or transmits PHI or performs certain functions, activities or services for or on behalf of UW Medicine, involving the use and/or disclosure of PHI.

2. **Protected Health Information** means health information that identifies the individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the individual, and that is transmitted or maintained electronically or in any other form or medium.

3. **Subcontractor** means a person or entity (other than a member of the BA’s workforce), to whom a BA delegates a function, activity or service, that creates, receives, maintains or transmits PHI.

4. **Workforce** means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or BA, is under the direct control of such covered entity or BA, whether or not they are paid by the covered entity or BA.

See UW Medicine Compliance Policy: PP00 Glossary of Terms.

**POLICY**

BAs are subject to the application of civil and criminal penalties under sections 1176 and 1177 of the Social Security Act and are directly liable for compliance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy, HIPAA Security Rule’s administrative, physical and technical safeguards and certain documentation requirements. UW Medicine is required to obtain satisfactory assurance that BAs appropriately safeguard PHI that may be created or received on its behalf. A BA may disclose PHI to a subcontractor, and may allow the subcontractor to create, receive, maintain or transmit PHI on the BA’s behalf, only if the BA obtains satisfactory assurance (a contract that meets the requirements of a BAA or other arrangement) that the subcontractor will appropriately safeguard the information and agree to the same restrictions and conditions that apply to the BA. PHI may be disclosed to a BA to create, receive, maintain or transmit PHI for or on behalf of the University of Washington or UW Medicine, not for independent use by the BA.
BA does not include:

1. A healthcare provider concerning the treatment of a patient;

2. A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting PHI for such purposes, to the extent such activities are authorized by law;

3. Activities or services for an organized healthcare arrangement; or

4. Courier services, such as the U.S. Postal Service or United Parcel Service and their electronic equivalents, such as internet service providers providing only data transmission services and who do not access the data other than on a random, or infrequent basis, as necessary to perform the transmission service or as required by law.

A. Satisfactory assurance

Before any disclosure of PHI is made to a BA, UW Medicine requires the BA to provide written assurances in the form of a BAA (see UW Medicine Business Associate Agreement, Attachment A).

UW Administrative Policy Statement 2.4 Information Security and Privacy Roles, Responsibilities, and Definitions requires that other than as allowed by law, when UW Medicine provides a third party access to or use of PHI, the contract or agreement must include terms and conditions that require compliance with applicable information security and privacy laws and University rules or policies. The UW Data Security Agreement (http://ciso.washington.edu/site/files/Data_Security_Agreement.pdf) may be used to meet this requirement with business partners, vendors, and other outside parties who are given UW confidential data.

An agreement or contract (Data Security Agreement) shall be used when one or more of the following scenarios occur:

1. UW Medicine transfers confidential data to a contractor’s offsite location;

2. Contractor accesses UW Medicine systems containing confidential data;

3. Contractor provides hardware or software support for UW Medicine systems and may have incidental access to confidential data;
4. Contractor provides hardware and/or software systems preconfigured to store or process confidential data. Reconfiguration may be constrained by the technical limitations of the hardware or software supplied by a contractor.

If any of the above scenarios occur, a Data Security Agreement must be included in addition to the BAA, as an addendum to the contract for the purchase of goods or services.

B. Required elements of a BAA

UW Medicine must document BA assurances in writing by executing an agreement with the BA. Such privacy and information security agreements are generally included in the contract between UW Medicine and the BA, although where both parties are government entities, a Memorandum of Understanding contains the privacy and information security agreement.

Required Elements

Every BAA must do four things:

1. Agree to be in compliance with all applicable laws, regulations, rules or standards, including, but without limitation, HIPAA, RCW 70.02 Medical Records – Health Care Information Access And Disclosure; RCW 19.255.010 Disclosure, notice – Definitions – Rights, remedies; and RCW 42.56.590 Public Records – Personal Information – Notice of Security Breaches.

2. Establish the permitted and required uses and disclosures of PHI by the BA (accurately describe how and why PHI is to be created, received, maintained and/or transmitted). A BAA may not authorize the BA to use or further disclose PHI except:

   a. To permit the BA to provide data aggregation services as needed for healthcare operations of the UW Medicine entity; or

   b. To permit the BA to use or disclose PHI if necessary for the proper management and administration of the BA, to carry out the legal responsibilities of the BA, or when the BA has: (1) obtained the third person’s assurances of confidentiality and no further use, and (2) the third person notifies the BA of any instances in which confidentiality is breached.

3. Require the BA to take and/or refrain from taking specific actions respecting the PHI. The BAA must:

   a. Prohibit any further use or disclosure of the information for any other purpose than that stated in the BAA or as permitted by law;
b. Require appropriate administrative, physical and technical safeguards to prevent use or disclosure of the information other than as provided in the BAA; and, to reasonably, and appropriately protect the confidentiality, integrity and availability of PHI that the BA creates, receives, maintains or transmits on behalf of UW Medicine. For example: controlling physical access to a computer or using security technologies for both paper and electronic records. Require deployment of appropriate safeguards to implement the Secretary of Health and Human Services’ annual guidance on the most effective and appropriate technical safeguards for use in carrying out security standards;

c. Require the reporting of any use or disclosure not provided for in the BAA to UW Medicine Compliance. The standard reporting requirement is within five business days, but not to exceed twenty days, of discovery;

d. Require the reporting of any Security Incident of which it becomes aware without unreasonable delay, within ten days, but not to exceed twenty days of discovery;

e. Require response to and reporting of any suspected or known security breach to UW Medicine Compliance; mitigate, to the extent practicable, harmful effects of security breaches known to the BA; and document security breaches and their outcomes. Unsecured PHI means PHI that is not rendered unusable, unreadable or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Health Information Technology for Economic and Clinical Health (HITECH) Act. The standard reporting requirement is within five business days, but not to exceed twenty days, of discovery;

f. Require that the BA supply UW Medicine Compliance with the following information to make notification:

- A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.

- A description of the types of unsecured PHI that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number or disability code).

- A brief description of what the BA is doing to investigate the breach, to mitigate losses, and to protect against any further breaches.

g. Require that the BA enter into a contract that meets the requirements of a BAA or other arrangement with 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;

h. Ensure that a subcontractor, to whom it provides such information, agrees to implement reasonable and appropriate safeguards to protect the information;

i. Require the BA to make PHI available in accordance with HIPAA and state laws governing access of individuals to PHI. See UW Medicine Compliance Policy: PP-23 Access of Individuals to Protected Health Information (PHI)/Designated Record Set;

j. Require the BA to make PHI available for amendment and to incorporate amendments in accordance with HIPAA and state law governing amendment of PHI. See UW Medicine Compliance Policy: PP-24 Amendment of Protected Health Information (PHI)/Designated Record Set;

k. Require the BA to record and report information to provide an accounting of disclosures in accordance with HIPAA and state law governing accounting of disclosures of PHI. See UW Medicine Compliance Policy: PP-25 Accounting of Disclosures of Protected Health Information;

l. Require the BA to restrict the disclosure of the PHI of an individual, if the Covered Entity agrees to a requested restriction by an individual. See UW Medicine Compliance Policy: PP-22 Rights to Request Additional Privacy Protection and Alternative Communications for Protected Health Information;

m. Require the BA to make available to the U.S. Department of Health and Human Services or its agents the BAs internal practices, books and records relating to the use and disclosure of PHI received from or created on behalf of a UW Medicine entity and cooperate with investigations and compliance reviews;

n. Require that, upon termination of the Agreement:

- The BA return or destroy all PHI received from or created on behalf of the UW Medicine entity and the BA is prohibited from retaining any copies of the PHI; or

- Where PHI is not destructible or returnable, the BA must extend the confidentiality protections and limit further uses and disclosures to only those purposes that makes returning or destruction infeasible.

4. Authorize termination of the BAA in the event of breach. UW Medicine must be allowed to terminate the BAA if the BA has committed a material breach or violated a provision of the BAA.
Additional Guidelines

1. Governmental entities

When the BA is a governmental entity, UW Medicine may enter into 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 BAA.

2. Legally required performance

If a BA is required by law to perform a function or activity on behalf of or in service to UW Medicine, then UW Medicine may disclose PHI to the BA as necessary without obtaining assurances in the form of a privacy agreement; provided, however, that UW Medicine undertakes a good faith attempt to ensure the BA implements appropriate safeguards. If the attempt to obtain written assurance fails, the UW Medicine entity must document the attempt and specify the reasons for the failure.

3. Compliance issues

When UW Medicine knows of a pattern of activity or practice that constitutes a material breach or a violation of the BA’s obligation under the BAA, UW Medicine must take reasonable steps to remedy the breach or end the violation. UW Medicine may terminate the agreement.

C. Violations of the BAA

1. Suspected or known violations

If a violation(s) of the BAA 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.

2. Substantiated violations

If the suspected violation is substantiated, the department manager or other individual initiating a contract works with purchasing to find an alternative BA to provide the goods or services and with purchasing and legal counsel to terminate the existing contract.

REGULATORY/LEGISLATION/REFERENCES

- 42 U.S. Code § 1320d-6 - Wrongful disclosure of individually identifiable health information
- 45 CFR Section 160.103 – Definitions.
- 45 CFR Section 164.104 – Applicability.
- 45 CFR Section 164.308 – Administrative Safeguards.
- 45 CFR Section 164.308 (a) (8) (b) (4) – Written Contract or Other Arrangements.
- 45 CFR Section 164.314 (a) – Business Associate Contracts or Other Arrangements.
- 45 CFR Section 164.500 – Applicability.
- 45 CFR Section 164.502 – Uses and disclosures of protected health information: general rules, paragraph (e) disclosures to business associates.
- 45 CFR Section 164.504 – Uses and disclosures: organizational requirements, paragraph (e) – business associate contracts.
- RCW 39.26 Procurement of Goods and Services
- RCW 42.56.590 Public Records – Personal Information – Notice of Security Breaches
- RCW 70.02 Medical Records – Health Care Information Access and Disclosure
- American Recovery and Reinvestment Act – Subtitle D Privacy
- Public Law 111–5 Section 13402(h) (2) HITECH Act.
- Fair and Accurate Credit Transactions Act of 2003

PROCEDURE ADDENDUM(s) REFERENCES/LINKS
- UW Medicine Compliance Policy: PP.00 Glossary of Terms
- UW Medicine Compliance Policy: PP-12 Attachment A - UW Medicine Business Associate Agreement
- UW Medicine Compliance Policy: PP-22 Rights to Request Additional Privacy Protection and Alternative Communications for Protected Health Information
- UW Medicine Compliance Policy: PP-23 Access of Individuals to Protected Health Information (PHI)/Designated Record Set
- UW Medicine Compliance Policy: PP-24 Amendment of Protected Health Information (PHI)/Designated Record Set
- UW Medicine Compliance Policy: PP-25 Accounting of Disclosures of Protected Health Information
- UW Administrative Policy Statement 2.10 Minimum Data Security Standards

ROLES AND RESPONSIBILITIES
Defined within POLICY.
### AUTHORITIES

<table>
<thead>
<tr>
<th>Custodian</th>
<th>Responsible Officer</th>
<th>Implementation Officer</th>
<th>Administrative Officer</th>
</tr>
</thead>
<tbody>
<tr>
<td>UW Medicine Compliance</td>
<td>UW Medicine Compliance</td>
<td>UW Medicine Compliance</td>
<td>UW Medicine Compliance</td>
</tr>
<tr>
<td><strong>Author</strong></td>
<td><strong>Owner</strong></td>
<td><strong>Auditor</strong></td>
<td><strong>Endorser</strong></td>
</tr>
<tr>
<td>UW Medicine Compliance</td>
<td>UW Medicine Compliance</td>
<td>UW Medicine Compliance</td>
<td>UW Medicine Executive Compliance Committee</td>
</tr>
</tbody>
</table>

### APPROVAL

UW Privacy Official  
Johnese M. Spisso, Chief Health System Officer,  
UW Medicine & Vice President for Medical Affairs, UW