Use and Disclosure of Protected Health Information by Business Associates

COMP.106

TABLE OF CONTENTS

Applicability: UW Medicine Affiliated Covered Entity

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

Policy Number: COMP.106

Superseded Policy: PP-12

Date Established: October 11, 2017

Date Effective: August 27, 2024

Next Review Date: August 27, 2027

PURPOSE

This policy outlines the criteria for a business associate (BA) relationship and establishes the requirements for disclosing protected health information (PHI) to a BA, including the required content of a Business Associate Agreement (BAA).

DEFINITIONS

See UW Medicine Compliance Glossary.

POLICY

A business associate (BA) is an outside entity or individual that is not part of the University of Washington or UW Medicine (or their workforce) that performs a service or activity for or on behalf of the University of Washington or UW Medicine that involves the use or disclosure of PHI.

A business associate does not include:

- A healthcare provider concerning the treatment of a patient;
- 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;
- Activities or services for an organized healthcare arrangement; *or*
- 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.

I. Disclosing PHI to a Business Associate

UW Medicine may disclose PHI to a BA only after a BAA is executed. The BA may only create, receive, maintain or transmit PHI for or on behalf of the University of Washington or UW Medicine. The BAA shall not allow the BA to use UW Medicine PHI for the BA's independent use unless such use is permitted or required by state or federal law.

II. Business Associate Agreement (BAA) Requirements

A. Prior to disclosing PHI to a BA, UW Medicine shall obtain satisfactory assurances in the form of an executed BAA that the BA will appropriately safeguard UW Medicine PHI.

B. If a BA is required by law to perform a function or activity on behalf of or in service to UW Medicine, UW Medicine may disclose PHI to the BA as necessary without obtaining assurances in the form of a written agreement only if UW Medicine undertakes a good faith attempt to ensure the BA implements appropriate safeguards. If the attempt to obtain written assurances fails, UW Medicine documents the attempt and specifies the reasons for the failure.

C. A UW Medicine 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 assurances that the subcontractor will appropriately safeguard the information and agree to the same restrictions and conditions outlined in the primary BAA with UW Medicine.

III. Determining the Need for a BAA

A. Department managers or other individuals initiating a contract or other business arrangement shall determine if the proposed arrangement meets the following three BA criteria:

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 perform 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 involve 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.)

B. If the proposed arrangement meets all three of the BA criteria, the other party is a UW Medicine BA, and the department manager or other individual initiating the agreement shall execute a BAA with the BA (see 106.T1 UW Medicine Business Associate Agreement). When the BA is a government agency, a Memorandum of Understanding may be executed instead of a BAA to document the satisfactory assurances. The Memorandum of Understanding shall contain the required elements of a BAA.

C. The signed BAA or Memorandum of Understanding shall be attached to and referenced in the underlying contract, if one exists, and a copy shall be provided to UW Medicine Compliance.

IV. Required Elements of a BAA

A. A BAA shall include the following elements as required by law:

1. A statement of agreement to comply with all applicable laws, regulations, rules or standards, including, but without limitation, HIPAA Privacy and Security Rules, 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 Act – Personal Information – Notice of Security Breaches.

2. The BA's specific permitted and required uses and disclosures of PHI (accurately describe how and why PHI is to be created, received, maintained and/or transmitted).

3. Prohibit the BA from any use or disclosure of the information other than as stated in the BAA or as required by law.

4. Require the BA to apply 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 electronic PHI that the BA creates, receives, maintains or transmits on behalf of UW Medicine.

5. Require the BA to report to UW Medicine Compliance any use or disclosure of the PHI not specified in the BAA (the standard reporting requirement is within five business days of discovery, but not to exceed twenty days);

6. Require the BA to report to UW Medicine Compliance any security incident of which it becomes aware without unreasonable delay (the standard reporting requirement is within ten days of discovery, but not to exceed twenty days);

7. Require the BA to report any suspected or known PHI breaches to UW Medicine Compliance (the standard reporting requirement is within five business days of discovery, but not to exceed twenty days);

8. Require the BA to respond to any suspected or known PHI breaches to mitigate, to the extent practicable, harmful effects of PHI breaches known to the BA;

9. Require the BA to document PHI breaches and their outcomes;

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

11. Require the BA to ensure that any subcontractors that create, receive, maintain or transmit PHI on behalf of the BA:

a. Enter into a contract or other arrangement with the BA that applies the same requirements in the BA's agreement with UW Medicine to the subcontractor, *and*
b. Agree to the same restrictions and conditions, including the implementation of reasonable and appropriate safeguards to protect the PHI, that apply to the BA;

12. Require the BA to make PHI available in accordance with HIPAA and state laws governing access of individuals to PHI;

13. Require the BA to make PHI available for amendment and to incorporate amendments in accordance with HIPAA and state laws governing amendment of PHI;

14. 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;

15. 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*;*

16. Require the BA to make available to the U.S. Department of Health and Human Services or its agents the BA's internal practices, books and records relating to the use and disclosure of PHI received from or created on behalf of a UW Medicine entity for purposes of determining UW Medicine's compliance with the HIPAA Privacy Rule;

17. Require that, upon termination of the Agreement:
    a. The BA shall return or destroy all PHI received from or created on behalf of the UW Medicine entity and prohibit the BA from retaining any copies of the PHI; *or*
    b. Where PHI is not destructible or returnable, the BA shall extend the confidentiality protections and limit further uses and disclosures of the PHI to those purposes that make the return or destruction of the PHI infeasible; and

18. Authorize termination of the BAA in the event of breach. UW Medicine must be allowed to terminate the agreement if the BA commits a material breach or violation of a provision of the BAA.

B. In addition, the BAA shall require the BA to pay the full costs of any required breach notice to affected individuals, including the costs to retain an outside consulting firm to undertake the notification effort. This requirement may be waived only through UW Medicine leadership approval.

C. A BAA shall not authorize the BA to use or further disclose PHI in a manner that would violate the regulations if done by UW Medicine except:

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

2. 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.

D. Signatory Authority

1. UW Medicine business associate agreements are signed in accordance with *Delegations of Authority for State Entities of UW Medicine*.

V. Violations of the BAA

A. Suspected or known violations

A workforce member who suspects or discovers a violation of a BAA shall report the matter to UW Medicine Compliance for investigation.

B. Substantiated violations

When UW Medicine confirms a pattern of activity or practice that constitutes a material breach or a violation of the BA's obligation under the BAA, UW Medicine shall take reasonable steps to remedy the breach or end the violation. If such steps are unsuccessful, UW Medicine shall terminate the agreement if feasible.

REGULATORY/LEGISLATION/REFERENCES

- Fair and Accurate Credit Transactions Act, Pub. L. 108-159 (November 2003).
- American Recovery and Reinvestment Act, Pub. L. 111-5, Title XIII, Subtitle D – Privacy.
- Notification in the Case of Breach, HITECH Act, 42 U.S.C. §17932.
- Wrongful Disclosure of Individually Identifiable Health Information, 42 U.S.C. § 1320d–6.
- General Provisions, 45 C.F.R. §160, Subpart A.
- Security Standards for the Protection of Electronic Protected Health Information, 45 C.F.R. § 164, Subpart C.
- Notification in the Case of Breach of Unsecured Protected Health Information, 45 C.F.R. §164, Subpart D.
- Privacy of Individually Identifiable Health Information, 45 C.F.R. §164, Subpart E.
- Revised Code of Washington (RCW) 19.255.010 Disclosure, Notice – Definitions – Rights, Remedies.
- RCW 39.26 Procurement of Goods and Services.
- RCW 42.56.590 Public Records Act – Personal Information – Notice of Security Breaches.
- RCW 70.02 Medical Records – Health Care Information Access and Disclosure.

PROCEDURE ADDENDUM(s) REFERENCES/LINKS

- UW Medicine Compliance Glossary.
- 106.T1 BAA Agreement.
- UW Administrative Policy Statement (APS) 2.2 University Privacy Policy.
- UW APS 2.4 Information Security and Privacy Roles, Responsibilities, and Definitions.
- UW APS 2.5 Information Security and Privacy Incident Reporting and Management Policy.
- Delegations of Authority for State Entities of UW Medicine.

ROLES AND RESPONSIBILITIES
Defined within POLICY.

APPROVAL

/s/ Beth DeLair
Beth DeLair,
Chief Compliance Officer, UW Medicine
Associate Vice President for Medical Affairs, UW

9/3/2024
Date