

University of Washington

PP-12 Attachment A
Rev.4/19/2016

Business Associate Agreement

This Agreement is entered into between the University of Washington (hereinafter “Covered Entity”) and _____ (hereinafter “Business Associate”). The University of Washington is a hybrid entity and has designated its healthcare components and non-healthcare components as described in UW Medicine Policy PP-01 Designation of Healthcare Components at the University of Washington. Pursuant to 45 CFR §164.103 and §164.105(a)(2)(iii)(C), the University’s designation includes the entities listed at http://depts.washington.edu/comply/docs/PP_01.pdf (hereinafter “Covered Entity”). This policy also lists the organizations with whom UW Medicine is in an organized healthcare arrangement. Business Associate includes any agents and subcontractors of the Business Associate that receive, create, maintain or transmit protected health information on behalf of the business associate.

This Agreement is incorporated into all existing and current contract(s) between the parties (the “Underlying Contract(s)”) under which Business Associate is carrying out activities or functions involving the use of protected health information (PHI), as this term is defined in 45 CFR Parts 160 and 164, and it replaces any prior agreement(s) entered concerning such PHI. Business Associates must reasonably and appropriately implement the standards and implementation specifications for safeguarding PHI and ensure the confidentiality, integrity, and availability of all electronic protected health information the business associate creates, receives, maintains, or transmits under federal Privacy and Information Security regulations (45 CFR Parts 160 and 164 (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH) Act) and are subject to the application of civil and criminal penalties under sections 1176 and 1177 of the Social Security Act and financial penalties under 45 CFR Sections 160.402, 160.404, 160.408, 160.410, 160.412, and 160.418. Business Associates must also comply with all requirements for protecting patient information under State Privacy regulations including but not limited to RCW 70.02. Covered Entity is committed to providing high quality patient care, education, and research. In furtherance of its mission, Covered Entity wishes to conduct transactions involving the disclosure of PHI to Business Associate for the purpose of conducting the activities set forth in the Underlying Contract(s).

Some or all of the information to be disclosed is required by law to be protected against unauthorized use, disclosure, modification or loss. In order to comply with applicable legal requirements for the protection of information, the parties agree as follows:

A. ALLOWABLE USES OF PHI

Only the minimum necessary PHI to accomplish the intended purpose of this agreement can be used or disclosed only for the following purposes (accurately describe how and why PHI will be created, received, maintained, and/or transmitted):

- 1.
- 2.
- 3.

B. OBLIGATIONS OF BUSINESS ASSOCIATE

Section 1. Safeguarding Information.

- A. Business Associate shall only use, store, disclose, or access PHI:
 - (1) In accordance with, and only to the extent permissible under the Underlying Contract; and
 - (2) In full compliance with all applicable laws, regulations, rules or standards, including, but without limitation HIPAA and RCW 70.02.

- B. Business Associate shall have in place policies and procedures to implement and maintain all safeguards necessary to ensure the confidentiality, availability, and integrity of all Covered Entity data. Business Associate shall deploy 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. Where applicable Business Associate shall report to the Covered Entity possible existence of identity theft (The Federal Trade Commission has regulations known as the Red Flag Rules which are part of the Fair and Accurate Credit Transactions (FACT) Act of 2003).

Section 2. Use or disclosure of Protected Health Information. Business Associate shall not use or disclose PHI received from Covered Entity in any manner that would constitute a violation of federal law, including but not limited to the Health Insurance Portability and Accountability Act of 1996 and any regulations enacted pursuant to its provisions ("HIPAA Standards"), or applicable provisions of Washington state law. Business Associate shall ensure that any use or disclosure by its directors, officers, employees, contractors, and agents of PHI received from Covered Entity, or created or received on behalf of Covered Entity is in accordance with the provisions of this Agreement and applicable federal and state law. Business Associate shall not use or disclose PHI in any manner other than that permitted or required by the Covered Entity for the purpose of accomplishing services to or on behalf of Covered Entity in accordance with the Underlying Contracts. Notwithstanding the foregoing, Business Associate may use PHI for the proper management and administration of the Business Associate and to carry out its legal responsibilities.

Section 3. Reporting Unauthorized Use or Disclosure of PHI. Business Associate shall, within five (5) working days of becoming aware of an unauthorized use or disclosure of PHI by Business Associate, its officers, directors, employees, contractors, agents or by a third party to which Business Associate disclosed PHI, report any such disclosure to Covered Entity. Such notice shall be made to the following:

UW School of Dentistry Compliance
Box 356365
Seattle WA 98195-6365
(206) 543-5331
dcomply@uw.edu

University of Washington

PP-12 Attachment A
Rev.4/19/2016

Business Associate Agreement

*****Use up to 60 Obligations. To the extent Business Associate is to carry out one or more of Covered Entity's obligations under Subpart E of 45 CFR Section 164, Business Associate will comply with the requirements of Subpart E that apply to Covered Entity in the performance of its obligations.

Section 5. Agreements by Third Parties. Business Associate shall enter into a contract or other arrangement with agents or subcontractor(s) to ensure that the same restrictions and conditions including the implementation of reasonable and appropriate safeguards to protect PHI that apply to the BA also apply to the agents or subcontractor(s).

Section 6. Access to Information. If Business Associate maintains Designated Record Set (DRS) documentation on behalf of Covered Entity, Business Associate agrees to provide access to the documentation maintained by the Covered Entity. Business Associate shall make available to Covered Entity such information for so long as it is maintained. If any individual requests access to PHI directly from Business Associate, Business Associate shall forward such request to the Covered Entity. Business Associate shall not deny any individual's request for access to the individual's PHI. A denial of access to PHI requested is the responsibility of the Covered Entity.

Section 7. Availability of PHI for Amendment. Within five days of a request from Covered Entity for the amendment of an individual's PHI or a record regarding an individual contained in a DRS (for so long as the PHI is maintained in the DRS), Business Associate shall provide such information to Covered Entity for amendment and incorporate any such amendments in the PHI as required by 45 C.F.R. §164.526.

Section 8. Accounting of Disclosures. Business Associate agrees to implement an appropriate record keeping and reporting process to enable it to provide the following information regarding disclosures of PHI: (i) the date of the disclosure, (ii) the name of the entity or person who received the PHI, and if known, the address of such entity or person, (iii) a brief description of the PHI disclosed, and (iv) a brief statement of the purpose of such disclosure which includes an explanation of the basis for such disclosure. If Business Associate receives a request for an accounting of disclosures, Business Associate shall forward such request to Covered Entity within a reasonable time frame to allow Covered Entity to prepare and deliver any required accounting of disclosures.

Section 9. Restrictions on Certain Disclosure of Health Information. Business Associate agrees to restrict the disclosure of the protected health information of an individual, if Covered Entity agrees to a requested restriction by an individual. If Business Associate receives a request for a restriction, Business Associate shall forward such request to Covered Entity within five business days to allow Covered Entity to respond to the requested restriction.

Section 10. Availability of Books and Records. Business Associate agrees to make its internal practices, books and records relating to the use and disclosure of PHI received from Covered Entity, or created or received on behalf of Covered Entity, available to the Secretary of the U.S. Department of Health and Human Services for purposes of determining Covered Entity's and Business Associate's compliance with the HIPAA Standards. Business Associate shall provide to Covered

University of Washington

PP-12 Attachment A
Rev.4/19/2016

Business Associate Agreement

Entity a copy of any documentation that Business Associate provides to the Secretary within five business days.

Section 11. Return or Destruction of Information. At the termination of the Underlying Contract(s), Business Associate shall return or destroy all PHI received from Covered Entity, or created or received on behalf of Covered Entity, that Business Associate maintains in any form. Business Associate will retain no copies of PHI. If Business Associate determines that return or destruction of any PHI is not feasible, Business Associate shall notify Covered Entity of the reasons why return or destruction is not feasible. If destruction or return of PHI is not feasible, Business Associate shall not use PHI received from Covered Entity, or created or received on behalf of Covered Entity, in a manner other than those permitted or required by state and federal laws or for the purposes described herein.

Section 12. Electronic Protected Health Information (“ePHI”). If Business Associate creates, receives, maintains or transmits ePHI on behalf of Covered Entity, Business Associate agrees to (1) implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of Covered Entity’s ePHI in accordance with Sections 164.308, 164.310, 164.312, and 164.316 of title 45, Code of Federal Regulations; (2) ensure that any third party agent or subcontractor who receives Covered Entity’s ePHI from Business Associate agrees to implement equivalent administrative, physical and technical safeguards; and (3) deploy 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; and (4) report any security breaches involving Covered Entity’s ePHI within five business days of discovery.

Section 13. Breaches Involving Unsecured PHI.

- A. A breach is when unsecured PHI may have been used, accessed, disclosed, or acquired in a manner not permissible under the terms of this Agreement. 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 Secretary in the guidance issued under section 13402(h)(2) of Public Law 111–5. If Business Associate has reason to believe that a breach has occurred, Business Associate will, within five business days of discovery, give Covered Entity notice. A breach shall be treated as discovered by the Business Associate as of the first day on which such breach is known to the Business Associate, (which includes any person, other than the individual committing the breach, who is an employee, officer, or other agent of the Business Associate) or should reasonably have been known to the Business Associate to have occurred. Business Associate shall give highest priority to immediately mitigate and remediate any unauthorized access and shall devote such resources as may be required to accomplish that goal. The Business Associate shall cooperate with all Covered Entity efforts, including providing any and all information necessary to enable Covered Entity to fully understand the nature and scope of the breach including but not limited to identification of each individual who has been affected by the breach.
- B. The Business Associate will investigate a breach of unsecured PHI to determine if the PHI has been compromised based upon a risk assessment in accordance with Section 164.402 (2).

- C. If it is determined that the PHI has been compromised, Covered Entity is required to provide notice to any or all individuals affected. In such case, Business Associate shall consult with Covered Entity regarding appropriate steps required to notify third parties. In the event that the Business Associate's assistance is required, such assistance shall be provided at no cost to Covered Entity and in accordance with the Covered Entity's policies and standards. Business Associate must coordinate with Covered Entity any public notification to any individual, media outlet, or the Secretary of Health and Human Services.
- D. If it is determined that notification is required, the Business Associate shall pay the full costs of notice to affected individuals, including the costs to retain an outside consulting firm to undertake the notification effort and will supply UW Medicine Compliance with the following information to make such notification:
- (1) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
 - (2) A description of the types of unsecured protected health information that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, or disability code).
 - (3) A brief description of what the Business Associate is doing to investigate the breach, to mitigate losses, and to protect against any further breaches.

Section 14. If the Underlying Contract does not include a provision for indemnification, then the Business Associate shall indemnify, hold harmless and defend Covered Entity from and against any penalties, claims, actions, loss, liability, damage, costs, or expenses, including but not limited to reasonable attorneys' fees.

Section 15. Covered Entity has the right, at any time, to monitor, audit, and review activities and methods in implementing this Agreement in order to assure compliance therewith, within the limits of Business Associate's technical capabilities.

Section 16. **Applicability to Organized Healthcare Arrangement (OHCA) Members.** To the extent that use or disclosure of any protected health information belonging to OHCA members, http://depts.washington.edu/comply/docs/PP_01.pdf is necessary to fulfill the terms of the Underlying Contract(s), Business Associate agrees to treat that information with the same level of confidentiality as Covered Entity's PHI and in accordance with the terms of this Agreement.

C. Miscellaneous.

Section 17. **Termination.** Notwithstanding any provision to the contrary in the Underlying Contract(s), Covered Entity may terminate its participation in the Underlying Contract(s) immediately upon written notice to Business Associate without liability for such termination, in the event that Covered Entity determines that Business Associate has committed a material breach or violated a provision of this Agreement.

Section 18. **Definitions.**

University of Washington

PP-12 Attachment A
Rev.4/19/2016

Business Associate Agreement

Personal Information means an individual's first name or first initial and last name in combination with any one or more of the following data elements:

- (a) Social security number;
- (b) Driver's license number or Washington identification card number; or
- (c) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

All terms not otherwise defined herein shall be defined in accordance with 45 CFR Parts 160, 162, and 164 and state laws governing healthcare privacy including but not limited to Public Records - Personal Information – Notice of Security Breaches (RCW 42.56.590), the Uniform Healthcare Information Act (RCW 70.02), mental illness (RCW 71.05), mental health services for minors (RCW 71.34), drug and alcohol abuse (RCW 70.96A, 42 CRF part 2), and HIV/AIDS/STDs (RCW 70.24).

Signature

Signature

UW SOD Representative Name
(School of Dentistry)

Business Associate Representative Name

Date

Date