



POLICY INFORMATION

Document # 900	Title: Business Associates and Business Associate Agreements	Original Effective Date: 9/7/2016
Safeguard: HIPAA Security Administrative	Approved by: Dean Beth E. Foley	Date Reviewed: 11/13/2017. 10/02/2019

I. POLICY STATEMENT

In accordance with CFR 45 §164.502, 164.504(e), 164.308, and 164.314, an HCC of CEHS may disclose Protected Health Information (PHI) to a Business Associate (BA) and may allow such individual or organization to create or receive such information on its behalf, if HCC obtains satisfactory assurances that the BA will appropriately safeguard the information. The HIPAA privacy regulations require satisfactory assurances to be provided in the form of a Business Associate Agreement (BAA) that contains certain elements specifically stated in the regulations.

It is the purpose of this policy to identify the process by which PHI can be appropriately released to Business Associates, and the mechanisms for developing and maintaining contractual agreements with Business Associates regarding their responsibilities and the HIPAA privacy regulations.

II. DEFINITIONS

See HIPAA Privacy Policy 100

III. AUTHORITY AND RESPONSIBILITIES

CEHS has component units that are listed as a hybrid entity in accordance with USU's HIPAA Hybrid Covered Entity Declaration. Only the Health Care Component/HCC (i.e., covered functions) of CEHS must comply with this policy. All references in this policy to "CEHS" shall be construed to refer only to the health care component of CEHS.

IV. PROCEDURES TO IMPLEMENT

Prior to allowing a HIPAA Business Associate access to CEHS Protected Health Information (PHI), the HCC must execute a Business Associate Agreement (BAA) with the BA. CEHS has developed a standardized BAA that has been approved by USU's Legal department that should be used. Changes to the BAA, must be reviewed and approved by the USU Legal department.

Where the HCC knows of a material breach or violation of the BAA by the BA, the HCC should notify and work with the Compliance Officer to take reasonable steps to cure the breach or end the violation. If such steps are unsuccessful, termination of the contract will be necessary. If

Emma Eccles Jones College of Education & Human Services

termination is not feasible, CEHS will work with the USU Privacy Officer to report the problem to HHS, Office for Civil Rights.

Members of the CEHS workforce must report suspected violations of the BAA by the BA to the Compliance Officer.

1. ACTIVITIES THAT REQUIRE A BUSINESS ASSOCIATE AGREEMENT - Each vendor or service provider that may receive, view, access, use, disclose or create PHI for the HCC must enter into a BAA in which it is obligated to protect the privacy and confidentiality of such information in accordance with the HIPAA privacy and security regulations. Examples of activities that require a BAA include:
 - a. Electronic Health Records (EHR) Vendor
 - b. Law firms/attorneys
 - c. External auditors or accountants
 - d. Shredding, destruction and/or documentation storage companies
 - e. Medical transcriptions services
 - f. E-prescribing gateways
 - g. Billing and coding vendors
 - h. Outside collection agencies
 - i. Consultants
 - j. Data processing firms or software companies that may collect, access, use, store or disclose PHI, or
 - k. Electronic applications, online back-up, cloud based software companies
 - l. Professional translator and interpretation services

HCCs are responsible for identifying any party outside of the covered entity that may access, use, disclose, view, or create PHI from the covered entity. If the business, service provider, vendor or individual will have access or have the potential to access PHI, the HCC will request a BAA. All signed BAA's shall be submitted through the USU document review process for approval. The HCC shall keep a copy of the signed agreement as well as provide one to the Compliance Officer.

2. CIRCUMSTANCES WHEN A BUSINESS ASSOCIATE AGREEMENT IS NOT REQUIRED -
 - a. A BAA is not required between other CEHS or USU HCCs.
 - b. A BAA is not required with members of the USU workforce or when a CEHS workforce member performs BA-type functions for the HCC in their capacity as a USU/CEHS workforce member.
 - c. Disclosures for treatment purposes between the HCC and healthcare providers including unaffiliated health care providers do not require a BAA.
 - d. Disclosure between the HCC and a financial institution for purposes of processing certain consumer financial transactions (credit card companies, banks, health insurance companies, etc.) do not require a BAA. Note: If the HCC initiates such payment activities it must meet the minimum necessary disclosure requirements.

V. ATTACHMENTS

Attachment A - CEHS Legal-Approved Business Associate Agreement

VI. REFERENCES

45 CFR §164.502(e)

45 CFR §164.504(e)

45 CFR §164.532(d-e)

45 CFR §164.308(b)(1)

45 CFR §164.314(a)

Attachment A



BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (“*Agreement*”) is made effective on _____ (“*Effective Date*”) by and between Utah State University (“USU”), on behalf of its _____ [Insert Name of Health Care Component] (“*Covered Entity*”) and _____ (“*Business Associate*”). Covered Entity and Business Associate each may be referred to herein as a “Party” or collectively as the “Parties.”

1. Purpose and Intent

Business Associate has entered into a certain Services Agreement to perform certain services for or on behalf of Covered Entity, which services may involve the Use or Disclosure of Protected Health Information within the meaning of the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) and its implementing regulations, 45 CFR Parts 160 and 164 (“the HIPAA Rules”), and the Health Information Technology for Economic and Clinical Health Act included in the American Recovery and Reinvestment Act of 2009 (the “HITECH Act”), as each of these may be amended from time to time. This Agreement supplements the Services Agreement defined herein and is intended to satisfy the requirements for Business Associate Agreements as set forth in the HIPAA Rules, including 45 CFR 164.50(e) and the HITECH Act. Business Associate hereby agrees to comply with applicable provisions the HIPAA Rules and the HITECH Act and to assist Covered Entity with its compliance as set forth herein.

2. Definitions. The following definitions apply to this Agreement:

2.1. “Services Agreement shall mean the _____ [effective date] _____ [Agreement Title] between USU and the Business Associate.

2.2. The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Individual, Minimum Necessary, Protected Health Information (see below), Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

2.3. “Business Associate” shall generally have the same meaning as the term “business associate” at 45 CFR 160.103, and reference the above-defined Party.

2.4. “Covered Entity” shall generally have the same meaning as the term “covered entity” at 45 CFR 160.103, and reference the above-defined Party.

2.5. “Protected Health Information” (PHI) means any information which is created or received by Business Associate from or on behalf of Covered Entity, whether oral or recorded in any form or medium, that relates to the past, present, or future physical or mental health or condition of an Individual, the provision of health care to an Individual, or the past, present, or future payment for the provision of health care to an Individual. See 45 CFR 160.103.

2.6. “HIPAA Rules” shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

Emma Eccles Jones College of Education & Human Services

2.7. “Security Standards” shall have the same meaning as the Security Standards at 45 CFR Parts 160, 162, and 164 and any implementing rules and regulations and in the HITECH Act.

3. Obligations and Activities of Business Associate

3.1. Non-Disclosure. Business Associate agrees to not use or disclose PHI other than as permitted or required by this Agreement or as Required by Law.

3.2. Safeguards. Business Associate agrees to use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic PHI, to prevent Use or Disclosure of PHI other than as provided for in this Agreement.

3.3. Reporting. Business Associate agrees to immediately report to Covered Entity any Use or Disclosure of the PHI not provided for by this Agreement of which it becomes aware, including Breaches of Unsecured PHI as required at 45 CFR 164.410, and any Security Incident of which it becomes aware.

3.4. Agents. In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any agent, including a Subcontractor, that creates, receives, maintains, or transmits PHI on behalf of Business Associate agrees to the same restrictions and conditions that to Business Associate with respect to such information.

3.5. Access. Upon a request by Covered Entity, Business Associate agrees to provide (in the time and manner designated by Covered Entity) access to PHI maintained in a Designated Record Set to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under 45 CFR § 164.524.

3.6. Amendments. Business Associate agrees to make any amendment(s) to PHI in a Designated Record Set as directed or agreed to by the Covered Entity pursuant to 45 CFR 164.526, or take other measures as necessary to satisfy Covered Entity’s obligations under 45 CFR 164.526.

3.7. Accounting of Disclosures. Business Associate agrees to maintain and make available the information required to provide an accounting of Disclosures to the Covered Entity or to an Individual as directed by the Covered Entity, as necessary to satisfy Covered Entity’s obligations under 45 CFR 164.528.

3.8. Delegated Obligations. To the extent the Business Associate is to carry out one or more of Covered Entity's obligation(s) under Subpart E of 45 CFR Part 164, Business Associate agrees comply with the requirements of Subpart E that apply to the Covered Entity in the performance of such obligation(s).

3.9. Inspection. Business Associate agrees make internal practices, books and records, including, but not limited to, policies and procedures and PHI, relating to the Use and Disclosure of PHI received from, or created or received by Business Associate on behalf of, Covered Entity available to the Covered Entity, or to the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the HIPAA Rules.

3.10. Required Disclosure. Business Associate agrees to immediately notify the Covered Entity in writing if Business Associate is Required by Law (including, but not limited to, by oral questions, interrogatories, requests for information or documents, subpoena, civil investigative demand, any informal or formal investigation by any government or governmental agency or authority or otherwise) to disclose any of the PHI. Business Associate agrees not to oppose any action by the Covered Entity to obtain a protective order or other appropriate remedy. If no such protective order or other remedy is obtained or the Covered Entity waives compliance with the terms of this Agreement, Business Associate will furnish only that portion of the PHI which it is advised by counsel is legally required and will exercise its reasonable best efforts to obtain reliable assurance that confidential treatment will be accorded the PHI;

3.11. HITECH Act. Business Associate agrees to comply with the requirements of the HITECH Act.

Emma Eccles Jones College of Education & Human Services

3.12. Mitigation. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a Use or Disclosure of PHI by Business Associate in violation of the requirements of this Agreement;

3.13. Policies and Procedures. Business Associate agrees to comply with the security policies and procedures adopted by the Covered Entity.

4. Permitted Uses and Disclosures by Business Associate

4.1. General Use and Disclosure Provisions. Subject to the terms and limitations of this Agreement and to the HIPAA Rules, HITECH Act, and any other application laws or regulations, Business Associate may use or disclose PHI on behalf of, or to provide services to, Covered Entity as necessary to perform the services in the Services Agreement, if such Use or Disclosure of PHI would not violate (1) the HIPAA Rules or HITECH Act if done by Covered Entity or (2) Covered Entity's policies and procedures which limit Disclosures to the Minimum Necessary. Except as specifically provided herein, all other uses or Disclosures of Covered Entity's PHI are not authorized by this Agreement and shall be prohibited. Business Associate may not use or disclose PHI in a manner that would violate Subpart E of 45 CFR Part 164 if done by Covered Entity, except for the specific Uses and Disclosures set forth below.

4.2. Specific Use and Disclosure Provisions. Subject to the terms and limitations of this Agreement and to the HIPAA Rules, HITECH Act, and any other application laws or regulations, Business Associate may, consistent with Covered Entity's policies and procedures:

- a. Disclose PHI as Required By Law;
- b. Use PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate;
- c. Use or disclose PHI for the proper management and administration of the Business Associate, provided that Disclosures are Required By Law or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached;
- d. Use PHI to provide Data Aggregation services to Covered Entity as permitted by 45 CFR § 164.504(e)(2)(i)(B).
- e. Use PHI to report violations of law to appropriate Federal and State authorities, consistent with 45 CFR § 164.502(j)(i).

5. Term and Termination

5.1. Term. The Term of this Agreement shall be effective as of Effective Date, and shall terminate upon termination of the Services Agreement or on the date Covered Entity terminates for cause as authorized in paragraph (b) of this Section, whichever is sooner.

5.2. Termination for Cause. Business Associate authorizes termination of this Agreement by Covered Entity, if Covered Entity determines Business Associate has violated a material term of the Agreement.

5.3. Obligations of Business Associate Upon Termination. Upon termination of this Agreement for any reason, Business Associate, with respect to PHI received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, shall:

- a. Retain only that PHI which is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities;
- b. Return to Covered Entity or, if agreed to by Covered Entity, destroy the remaining PHI that the Business Associate still maintains in any form;

Emma Eccles Jones College of Education & Human Services

c. Continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to electronic PHI to prevent Use or Disclosure of the PHI, other than as provided for in this Section, for as long as Business Associate retains the PHI;

d. Not use or disclose the PHI retained by Business Associate other than for the purposes for which such PHI was retained and subject to the same conditions set forth in this Agreement which applied prior to termination; and

e. Return to Covered Entity or, if agreed to by Covered Entity, destroy the PHI retained by Business Associate when it is no longer needed by Business Associate for its proper management and administration or to carry out its legal responsibilities.

The obligations of Business Associate under this Section shall survive the termination of this Agreement.

6. **Miscellaneous**

6.1. Choice of Law and Venue. The Agreement will be governed by the laws of the State of Utah, without regard to conflicts of laws principles. Venue for any lawsuits, claims, or other proceedings between the Parties relating to or arising under the Agreement shall be exclusively in the State of Utah.

6.2. Interpretation. Any ambiguity in this Agreement, including the agreements referenced in Section 3 above, shall be resolved to permit the Covered Entity to comply with the HIPAA Rules, the HITECH Act, the Security Standards, and all applicable laws and regulations.

6.3. Civil and Criminal Liability. HIPAA's civil and criminal administrative simplification penalties for data security and privacy shall apply to the Business Associate to the same extent that those penalties apply to the Covered Entity.

6.4. No Third-Party Beneficiaries. Nothing express or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than Covered Entity, Business Associate, and their respective successors and assigns, any rights, remedies, obligations or liabilities whatsoever.

6.5. Indemnification. Business Associate agrees to release, indemnify, and hold harmless USU, its trustees, officers, agents, employees, students, and volunteers ("Indemnitees") from and against all liability, including claims, demands, losses, damages and expenses of every kind and description to persons (including death) or property arising directly or indirectly from the acts or omissions of Business Associate. Such indemnification includes, but is not limited to, attorney's fees, court costs, mediation/arbitration costs, as well as costs of damage to property of expenses of every kind resulting from Business Associate's actions or omissions. This provision shall bind any and all successors, assigns, agents, employees, heirs, personal representatives, or anyone else claiming to represent Business Associate. USU shall not be liable for any special, consequential, lost profit, expectation, punitive or other indirect damages in connection with any claim arising out of or relating to this Agreement, whether grounded in tort (including negligence), strict liability, contract, or otherwise. In the event a dispute between the Parties results in litigation, in addition to any other relief to which may be entitled, the prevailing party shall be reimbursed for reasonable attorney fees and other reasonable costs.

6.6. Government Records and Management Act. Business Associate acknowledges that USU is a governmental entity subject to the Utah Government Records Access and Management Act, Utah Code Ann., Section 63G-2-101 et seq., as amended ("GRAMA"); that certain records within USU's possession or control, including without limitation, the Agreement (but not including PHI), may be subject to public disclosure; and that USU's confidentiality obligations shall be subject in all respects to compliance with GRAMA. Pursuant to Section 63G-2-309 of GRAMA, any confidential information, other than PHI, provided to USU that Business Associate believes should be protected from disclosure must be accompanied by a written claim of confidentiality with a concise statement of reasons supporting such claim. Notwithstanding any provision to the contrary in the Agreement, USU may disclose any information or record to the extent required by GRAMA or otherwise required by law, and to USU's employees, attorneys, accountants, consultants and other

Emma Eccles Jones College of Education & Human Services

representatives on a need to know basis; provided, that such representatives shall be subject to confidentiality obligations no less restrictive than those set forth in the Agreement.

6.7. Governmental Immunity. Business Associate further acknowledges that USU is a governmental entity under the Governmental Immunity Act of Utah, Utah Code Ann., Section 63G-7-101 et seq., as amended (the "Act"). Nothing in the Agreement shall be construed as a waiver by USU of any protections, rights, or defenses applicable to USU under the Act, including without limitation, the provisions of Section 63G-7-604 regarding limitation of judgments. It is not the intent of USU to incur by contract any liability for the operations, acts, or omissions of Business Associate or any third party and nothing in the Agreement shall be so interpreted or construed. Without limiting the generality of the foregoing, and notwithstanding any provisions to the contrary in the Agreement, any indemnity obligations of USU contained in the Agreement are subject to the Act and are further limited only to claims that arise directly and solely from the negligent acts or omissions of USU. Any limitation or exclusion of liability or remedies in the Agreement for any damages other than special, indirect or consequential damages, shall be void and unenforceable.

6.8. USU Insurance. USU carries insurance through the State Risk Manager of the State of Utah up to the limits required by the State Risk Manager and applicable law. Nothing in the Agreement shall require USU to carry different or additional insurance, and any obligations of USU contained in the Agreement to name a party as additional insured shall be limited to naming such party as additional insured with respect to USU's negligent acts or omissions.

6.9. Notice. Any payment, notice, or other communication required or permitted to be given to either party hereto shall be in writing and shall be deemed to have been properly given and effective: (a) on the date of delivery if delivered in person during recipient's normal business hours; or (b) on the date of attempted delivery if delivered by courier, express mail service or first-class mail, registered or certified. Such notice shall be sent or delivered to the respective addresses listed in the opening clause of this Agreement.

6.10. Assignment. Neither Party may assign, transfer, or otherwise dispose of its rights, interests, or duties hereunder, in whole or in part, to any third party without prior written approval from the other Party.

6.11. Relationship of Parties. In assuming and performing the obligations of this Agreement, the Parties are each acting as independent parties and neither shall be considered or represent itself as a joint venture, partner, agent, or employee of the other.

6.12. Amendment and Supplement. Any amendment and/or supplement of this Agreement shall come into force only after a written agreement is signed by both Parties; provided, however, that this Agreement may be amended from time to time by the Covered Entity to comply with the requirements of the HIPAA Rules, the HITECH Act, the Security Standards, and associated implementing regulations. Any such compliance-related amendment shall be in writing and signed by Business Associate. The amendment and supplement duly executed by both Parties shall be part of this Agreement and shall have the same legal effect as this Agreement.

6.13. Merger. This Agreement embodies the entire understanding of the Parties and supersedes all previous communications, representations, or understandings, either oral or written, between the Parties relating to the subject matter thereof.

6.14. Severability. The provisions of this Agreement are severable, and in the event that any provision of this Agreement shall be determined to be invalid or unenforceable under any controlling body of the law, such invalidity or unenforceability shall not in any way affect the validity or enforceability of the remaining provisions herein.

IN WITNESS THEREOF the Parties have caused this Agreement to be duly executed on their behalf by a duly authorized representative as of the Effective Date set forth above.

UTAH STATE UNIVERSITY

BUSINESS ASSOCIATE

By: _____

By: _____

Emma Eccles Jones College of Education & Human Services

Print Name:

Title:

Date: _____

Print Name:

Title (if applicable):

Date: _____

Effective Date: 11/9/2017