PROCEDURE 2202-PR7
Business Associate Relationships with Vendors

Associated Policy: Policy 2202, Privacy and Security of Protected Health Information Under HIPAA
Effective Date: 2024/11/08
Latest Revision: 2024/11/08
Category: Community Expectations
Subcategory: Records

POLICY STATEMENT (POLICY 2202.2.7)

"Contractors and/or vendors that have access to PHI while providing certain services, functions or activities for a Health Care Component (HCC) at USU must enter into a Business Associate Agreement (BAA) governing the use, maintenance, and disclosure of PHI. The agreement shall set forth appropriate safeguards for the PHI it receives or creates on behalf of the covered entity. When possible, HCCs shall use the HIPAA Business Associate Agreement Template, available at USU's HIPAA website."

PURPOSE

The purpose of this procedure is to provide instructions to HCCs – including USU units that would otherwise be considered Business Associates (BAs) if they were not business units of the university – in developing BAAs and provisioning individuals for use of systems that are subject to BAAs.

DEFINITIONS

Definitions in this Procedure shall be as set forth in Definitions Document 2202-D1, *Definitions that Apply to Protected Health Information under HIPAA*.

PROCEDURES

1. BAAs initiated by HCCs that are Health Care Providers or Health Plans

When a Business Associate (BA) is being engaged directly by a HCC that is either a healthcare provider or a health plan (see "Designation of Health Care Covered Components" in USU's Hybrid Entity), the business case for the engagement must include that the HCC plans to provide PHI to the BA in order for the BA to effectively carry out its supporting function for the HCC. In such cases, the HCC shall initiate a BAA, using the standard USU BAA template whenever feasible. All BAA's are legal agreements, and must be reviewed and approved using the ServiceNow system for contract reviews. No BAA may be entered into or renewed without having been reviewed and approved by USU's Office of General Counsel. BAA's may provide sufficient guidance for some arrangements between HCCs and BAs, but may also be coordinated with other service agreements with BAs. All such agreements shall be reviewed through ServiceNow, or other review protocols as may be implemented from time to time by USU.

2. BAAs initiated by HCCs that are units that provide services to providers and health plans

When a USU business unit that supports HCCs that are health care providers or health plans, those business units become part of USU's HCC (see listing under "Business Support Covered Components" in the "Designation of Health Care Covered Components). In that role, these units may develop, implement and support relationships with third party vendors to provide systems and applications that enhance USU services to its employees and clientele. In these situations, BAA's may be executed with vendors if a business need exists for those systems to create, store or transmit PHI. BAAs implemented via this workflow shall be initiated separately from the underlying contract for the third-party service, and shall be reviewed and approved using the same Service Now system. In these cases, the Office of General Counsel, the HIPAA Privacy Officer and HIPAA Security Officer shall be included as reviewers. The BAA

shall be maintained by the unit that maintains the vendor relationship. USU HIPAA privacy officers shall have responsibility to coordinate the use of BAA-provisioned systems with USU health care providers and health plans within their units.

3. Provisioning of users who create, store or transmit PHI within BAA compliant systems

It will remain the responsibility of each HCC to train employees and provision them for use of systems and devices that create, store or transmit PHI. Each HCC shall maintain an inventory of its employees who handle PHI, and shall map PHI held within the unit to each system where PHI resides. HCCs may, within the parameters of existing policies and procedures, utilize any third-party system that has a current BAA with USU to create, store or transmit PHI; however, each unit may also choose not to allow use of such systems in order to provide appropriate controls to protect PHI. Units are encouraged to refer to Knowledgebase documents including Data Storage Quick Reference (https://usu.service-now.com/kb_view.do?sysparm_article=KB0014909) and Data Classification Quick Reference (https://usu.service-now.com/kb_view.do?sysparm_article=KB0014821) and to interface with divisions and offices that maintain the systems while preparing training materials.

4. Granting exceptions

When units require the use of unit-designated systems when creating, using, storing and disclosing PHI, all PHI-impacted activities shall be conducted using those systems unless justification for use of a separate BAA-provisioned system is provided and accepted by unit management for an exception. All exceptions shall be approved at least at the unit management level. Exceptions shall be granted after a risk assessment is completed and a risk mitigation plan is approved by the unit's HIPAA Security Officer. All exceptions shall be term-limited, but renewable at the discretion of the unit manager and the HIPAA Security Officer.

5. Deprovisioning of users

Immediate deprovisioning of former employees when they are no longer authorized to access PHI is crucial to protecting PHI and reducing USU's compliance risks. Only in exceptional circumstances may former students or employees retain access to any PHI held at USU. Such exceptions shall be approved by the unit and by a dean or vice president, and reasonable efforts shall be made to limit access as soon as possible. Units should consider use of limited data sets, or limiting access to deidentified data in these situations.

Former employees should be notified immediately when they are no longer authorized to access PHI or other restricted data. Coordination with the unit(s) that administer all systems used by terminated individuals is required in order to expeditiously de-credential them from each system they utilized. Credentialing and de-credentialing of individuals either manually or through an automated system is acceptable. In either case, adequate documentation of deprovisioning shall be maintained to demonstrate the continuous integrity of USU's systems, and to ensure that PHI-impacted systems are not subject to inappropriate uses or disclosures which may rise to unallowable breaches of the system.

HISTORY

2022/11/03 New number assigned