

Business Associate Agreements

HIPAA Guidance - 06



About This Guidance

Effective: 07/01/2017

Last Updated: 12/13/2021

Responsible University Office:

Office of the Chief Privacy Officer

Responsible University Administrator:

Chief Privacy Officer

mawerlin@iu.edu

Guidance Contact:

HIPAA Privacy Officer

HIPAA Security Officer

hipaa@iu.edu

Scope

This guidance applies to the workforce members in the designated Indiana University (IU) HIPAA Covered Healthcare Components and HIPAA Affected Areas, anyone rendering services as a Business Associate, and anyone who creates, receives, maintains, or transmits Protected Health Information (PHI) in any capacity at IU, including, but not limited to, faculty, staff, students, trainees, volunteers, visiting scholars, and third-party agents. For the purposes of this policy, all of the above will be referred to as workforce members.

Guidance Statement

A. IU as the Covered Entity

1. Business Associates of IU are required to enter into a Business Associate Agreement (BAA), or the BAA required language is to be added to a service agreement which outlines the responsibilities of the Business Associate with respect to the use, disclosure, and safeguarding PHI.
2. Activities of the Business Associate will be managed through the BAA. The BAA is completed during the procurement process. If the Business Associate fails to fulfill its responsibilities outlined in the BAA there may be an opportunity to correct the failure. If the failure is not corrected the contract may be terminated.
3. The Business Associate may provide PHI to a "subcontractor" if the Business Associate and subcontractor have entered into an agreement that meets the requirements of the IU BAA ensuring the same restrictions and conditions for implementing appropriate safeguards to protect PHI apply to the subcontractor.
4. Suspected or discovered violations of a BAA should be reported to the IU incident response team (it-incident@iu.edu) and the University HIPAA Privacy Officer to investigate.
5. Examples of instances when a BAA is necessary:
 - a. Data processing or software companies that have access to computer systems or databases containing PHI, including cloud based services
 - b. Accreditation organizations

- c. Record storage facilities or shredding services*
- d. Consulting services
- e. Temporary employment agencies that place individuals in positions where they will have access to PHI
- f. Lawyers, accountants, external auditors, translator services, consultants

*IU has university-wide agreements with vendors for this purpose and the agreements must include a BAA when PHI is involved.

- 6. All IU vendors that have access to IU data classified as critical, including PHI must go through an approval process, IU's third-party security review.
- 7. BAAs are to be retained in the appropriate contract management system by Purchasing, General Counsel, or the Office of Research Administration (ORA) for six years following the termination of the agreement.

B. IU as the Business Associate

- 1. In some instances, IU may receive or create PHI to perform a service on behalf of an external covered entity. In those cases, IU may be a Business Associate and may be required to enter into a Business Associate Agreement (BAA) with that covered entity.
- 2. Activities of IU as the Business Associate will be managed through the covered entity's BAA. The BAA may be requested during the contract, grant or service agreement phase of the engagement.
- 3. IU as the Business Associate may provide PHI to a "subcontractor" if IU and the subcontractor have entered into an agreement that meets the requirements of the BAA ensuring the same restrictions and conditions for implementing appropriate safeguards to protect PHI apply to the subcontractor.
- 4. Suspected or discovered violations of a BAA should be reported to the IU incident response team (it-incident@iu.edu) and the University HIPAA Privacy Officer to investigate.
- 5. Examples of instances when IU may be a business associate:
 - a. Providing data processing services, hardware and/or software support, or colocation services that involve systems containing PHI, including IU provided cloud based services;
 - b. Consulting services;
 - c. Management of non-IU research projects that involve PHI;
 - d. Management of projects for the Indiana Department of Public Health, Indiana Medicaid or other state or county agencies when the project involves PHI.
- 6. IU's HIPAA Privacy Officer is to be notified of any service arrangement in which IU may be a Business Associate, to review the arrangement and BAA prior to signing.
- 7. BAAs are to be retained in the appropriate contract management system by Purchasing, General Counsel, or the Office of Research Administration (ORA) for six years following the termination of the agreement.

C. Signature Authority

- 1. Only the Treasurer of the Trustees of Indiana University and others acting in conjunction with the Treasurer are granted specific authority to execute certain documents on behalf of the University, including BAAs.
- 2. The Treasurer has the sole authorization to delegate authority and has delegated Signature Authority for Business Associate Agreements to the following:
 - a. Executive Director of Procurement Services and sub-delegated staff;

Reason for the Guidance

IU is required to identify vendors who qualify as Business Associates as defined by the Privacy and Security Rules of the HIPAA regulation and the HITECH Act to ensure that PHI is being appropriately safeguarded by third parties.

When IU is a Business Associate of another covered entity, IU will be required to enter into an agreement and must comply with the HIPAA Security Rule, portions of the HIPAA Privacy Rule that apply to the service being provided as well as the requirements in the covered entity's Business Associate Agreement.

Definitions

Business Associate: An individual or entity who performs certain functions or activities on behalf of IU that involve the use or disclosure of PHI. Business associate functions and activities include: claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; practice management; and repricing. Business associate services are: legal; actuarial; accounting; consulting; data aggregation; management; administrative; accreditation; and financial. A covered entity may be a business associate of another covered entity.

See [Glossary of HIPAA Related Terms](#) for complete list of terms.

History

07/01/2017 Effective Date
02/12/2018 Updated
12/13/2021 Updated contact information, signature authority

Related Information

HIPAA-P01 Uses & Disclosures of Protected Health Information Policy
HIPAA-P02 Minimum Necessary Policy