

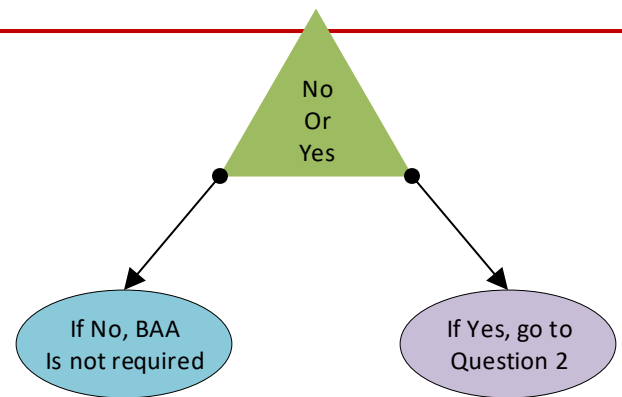
HIPAA/HITECH Business Associate Agreement Decision Tree

HIPAA regulates the use and disclosure of information between a covered entity and a business associate. A business associate is a person or entity, other than a workforce member, who creates, receives, maintains, or transmits PHI on behalf of a covered entity, or who provides services to or for the covered entity which involve the disclosure of protected health information.

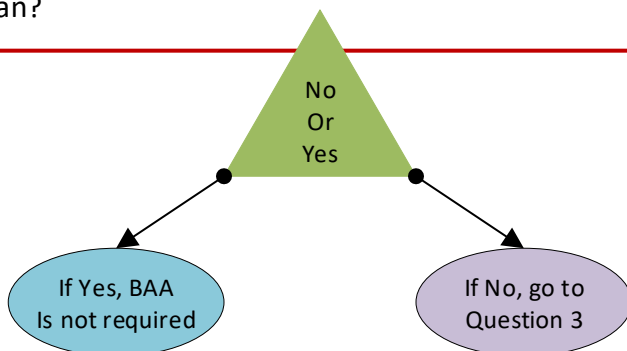
This BAA Decision Tree is provided to assist in the process of identifying when a Business Associate Agreement is necessary; however, the HIPAA rule has many complicated details and exceptions which may require additional analysis. Please contact the Privacy Office with questions.

Question 1 – Is Protected Health Information (PHI) being disclosed to a person or entity outside of the UofL workforce? “Workforce” includes employees, contractors, volunteers, trainees, and students.

Generally speaking, *protected health information (PHI)* is information in any form (verbal, electronic, or written) that is held by a covered entity or its business associate that identifies a person and relates to the person’s past, present, or future physical or mental condition or relates to payment of the person’s health care services.



Question 2 – Is PHI being disclosed to any of the following: a health care provider for treatment purposes, **OR** to a health plan for payment purposes, **OR** to a health plan sponsor with respect to disclosures by a group health plan?

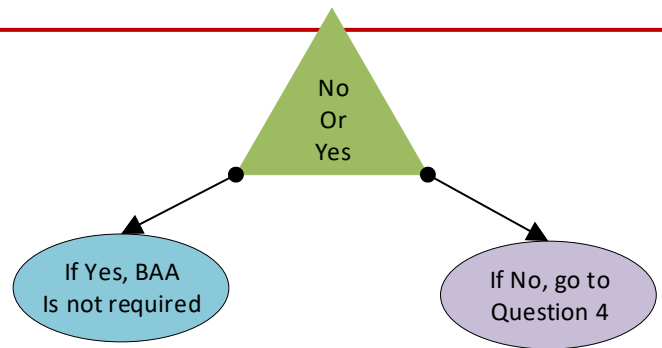


Examples of disclosures for treatment purposes include providing PHI to primary/referring physicians, contract physicians or specialists, contract nursing staff, contract rehab staff, ambulances, home health agencies, dentists, and hospitals.

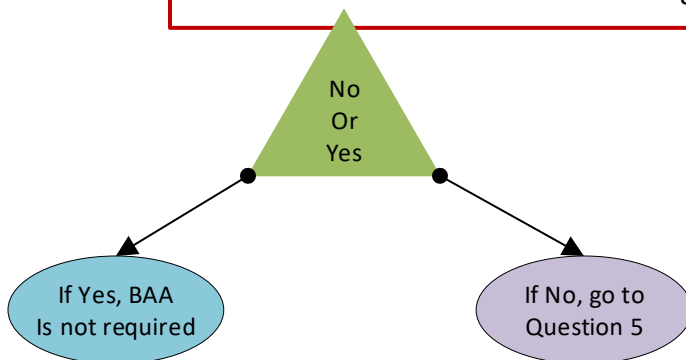
HIPAA/HITECH Business Associate Agreement Decision Tree

Question 3 – Is the PHI being disclosed to a government agency pursuant to an official investigation (e.g., CMS, OCR, OSHA, FDA, Health Department, etc)?

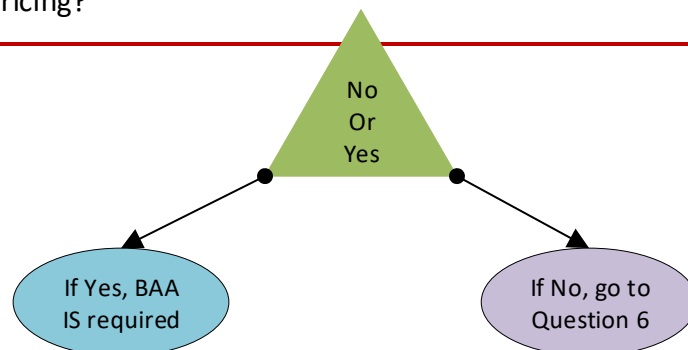
The Privacy Rule permits disclosure of PHI to law enforcement officials, without an individual's authorization, **under specific circumstances**. Contact the Legal Department or Privacy Office for assistance or questions regarding official investigations or legal proceedings.



Question 4 – Is the PHI being disclosed to another covered entity that is part of an organized healthcare arrangement in which the originating covered entity participates?



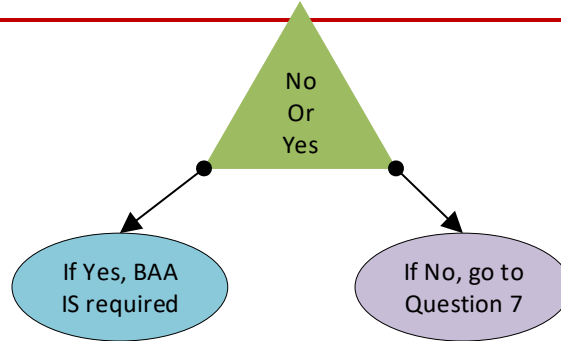
Question 5 – Does the other person or entity create, receive, maintain or transmit PHI **on behalf of** the covered entity for a function or activity regulated by HIPAA, including: claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities, billing, benefits management, practice management, and repricing?



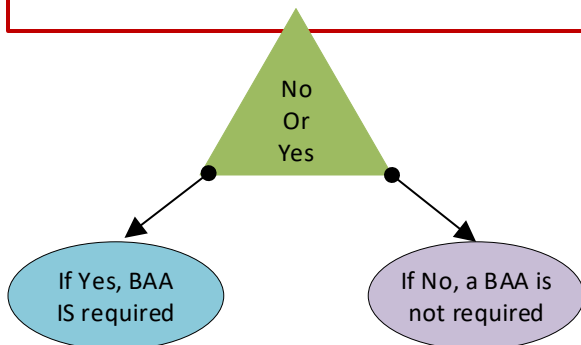
This BAA Decision Tree is provided to assist in the process of identifying when a Business Associate Agreement is necessary; however, the HIPAA rule has many complicated details and exceptions which may require additional analysis. Please contact the Privacy Office with questions.

HIPAA/HITECH Business Associate Agreement Decision Tree

Question 6 – Does the other person or entity provide legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services **on behalf of** the covered entity where the provision of such services involves disclosure of PHI to the person or entity?



Question 7 – Will the other person or entity be able to access PHI on a routine basis, AND/OR is there a possibility that the PHI in the person or entity's custody or control could be compromised (e.g., data storage vendor, document shredding company, etc)?



For Questions 6, 7, & 8

HITECH specifically includes the following entities:

- * Health Information Organizations
- * E-prescribing gateways
- * Data transmission vendors with routine access to PHI
- * Personal Health Record vendors that offer a PHR to individuals on behalf of a covered entity
- * Subcontractors that create, receive, maintain, or transmit PHI for or on behalf of a business associate

This BAA Decision Tree is provided to assist in the process of identifying when a Business Associate Agreement is necessary; however, the HIPAA rule has many complicated details and exceptions which may require additional analysis. Please contact the Privacy Office with questions.