

Who can assess private health information under HIPAA?

Key Points from the Feds:

1. **Minimum Necessary Requirement:** Protected health information should not be used or disclosed when it is not necessary to satisfy a particular purpose or carry out a function related to job duties. Visit: <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/minimum-necessary-requirement/index.html>
2. **Definition of a privacy breach:** “The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users, for other than authorized purpose, have access or potential access to personally identifiable information, whether physical or electronic.” Visit: https://www.cms.gov/Research-Statistics-Data-and-Systems/Computer-Data-and-Systems/Privacy/Privacy_Data_Breach.html
3. **The most frequent HIPAA violation** leading to investigations, according to the Feds: Impermissible uses and disclosures of PHI. Visit: <https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html>

Who is a Business Associate under HIPAA?

Key Points from the Feds:

1. **A Business Associate** is any outside person or company who may have *potential* access to protected health information (PHI). Visit: <https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html>
2. **What is a Business Associate Agreement (BAA)?**: A Business Associate Agreement is a signed contract that places responsibility on a Business Associate for protecting private health information. A BAA essentially requires an outside contractor to meet all privacy and security standards set forth under HIPAA. Visit: <https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html>
3. **Liability of Business Associates**: A May 2019 Fact Sheet, issued by the Office of Civil Rights, announced that the Feds may pursue violations against Business Associates only -- meaning the contracting agency does not need to be part of the inquiry. "Impermissible uses and disclosures of PHI" is specified as justification for initiating such an investigation. Visit: <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/factsheet/index.html>