

MYTH: A Business Associate Agreement is required when a covered entity contracts with an external Institutional Review Board (IRB).**FACT: Even if the IRB is an external organization, not part of the covered entity, the IRB is not a business associate if its functions are limited to review, approval, and oversight of research.**

An Institutional Review Board (IRB) is a “board, committee, or other group formally designated by an institution to review, to approve the initiation of, and to conduct periodic review of biomedical research involving human subjects. The primary purpose of such review is to assure the protection of the rights, safety, and welfare of human subjects.”¹ IRBs are typically made up of employees of the institution they serve (such as a hospital or university) as well as community volunteers. However, some institutions contract with external IRBs that are not part of the institution and whose members are not employees of the institution doing the research. IRB review or waiver is required for research under HIPAA, as well as other research involving human subjects.

When the HIPAA Privacy and Security Rules were revised in light of the HITECH Act, there was concern that the new rules extending direct liability to business associates would apply to external IRBs, which frequently handle protected health information (PHI) in the course of their reviews.

In general, covered entities (health care providers, health plans, or clearinghouses) must enter into business associate agreements when they intend to share PHI with an external organization that

creates, receives, maintains, or transmits PHI on behalf of a covered entity for specific business functions (such as claims processing, data analysis, utilization review, quality assurance, and billing) or for the provision of professional services (such as legal, accounting, data aggregation, etc). The final HIPAA regulations make clear that, just as a covered entity may contract with an external researcher for authorized research purposes, “an external or independent institutional review board is not a business associate of a covered entity by virtue of its performing research review, approval and continuing oversight functions.”² However, if the external IRB provides any other regulated functions, such as management or consulting, it may be a business associate by virtue of those additional functions, in which case a business associate agreement would be required for the use and exchange of PHI.

For More Information:

- [See](#) our Fast Facts about business associates under HIPAA.
- [Use](#) our Decision Support Tool to determine if you are a business associate.
- [Learn](#) about state and federal laws related to health information privacy and confidentiality.

Follow us on Twitter at [@HealthInfoLaw](#)

¹ 21 CFR § 56.

² 78 Fed. Reg. 5575.