Thoropass™

HIPAA vs HITRUST: Navigating the World of Healthcare Information Security

If you work in the healthcare industry, you know protecting sensitive health information is crucial. There are several frameworks and standards in place to help organizations ensure the security of this information, but it can be confusing to understand the differences between them. This post will specifically address the differences between HIPAA (Health Insurance Portability and Accountability Act) and HITRUST (Health Information Trust Alliance).

Differences between HIPAA and HITRUST

HIPAA is a federal regulation setting standards for protecting personal health information. It applies to covered entities, such as healthcare providers, health plans, and healthcare clearinghouses, and is enforced by the Department of Health and Human Services (HHS) as well as the Attorney Generals from each state. Compliance with HIPAA is mandatory for covered entities, and non-compliance can result in fines and legal action. Notably, under HIPAA, a service provider to a covered entity becomes a "Business Associate" if the service provider provides certain services to a covered entity involving the use or disclosure of protected health information (PHI). A business associate is any organization that creates, receives, maintains, or transmits protected health information on behalf of a covered entity. (Maintaining also includes the persistence of custody over the information, which brings in cloud service providers who never use or disclose PHI.)

HITRUST, on the other hand, is a voluntary third-party certification organizations can obtain to demonstrate their commitment to protecting sensitive information. While HITRUST is not a government regulation, it's based on many regulatory and industry standards, including HIPAA. Obtaining HITRUST certification requires a more comprehensive set of requirements and a more thorough evaluation process than HIPAA.

Evaluating compliance with HIPAA and HITRUST

An assessor may use the Office for Civil Rights (OCR) Audit Protocol, developed by the HHS's Office for Civil Rights, to provide guidance for assessing an organization's implementation of HIPAA requirements. If violations of the regulations are alleged, HHS determines HIPAA compliance through audits and investigations.

HITRUST compliance is evaluated through a formal certification process. Organizations seeking HITRUST certification must undergo a comprehensive assessment by a HITRUST-approved assessor. If the organization is found to be compliant with the HITRUST framework, the results will be submitted to HITRUST, who may grant HITRUST certification.

Reporting on Compliance with HIPAA and HITRUST:

One key difference between HIPAA and HITRUST is the way in which assurance is gained. Under HIPAA, assurance is typically gained through a Business Associate Agreement (BAA), an assessment report, or a SOC 2+ report. A BAA is a legally binding contract between a healthcare organization and a business associate outlining the responsibilities and obligations of both parties in regards to protecting patient data. An assessment report is a document providing a detailed assessment of an organization's compliance with HIPAA regulations, and a SOC 2+ report is a type of security assessment that evaluates an organization's controls under the audit guidance published by the American Institute for Public Accountants (AICPA).

HIPAA reporting is nuanced and organizations should work with professionals who have expertise in assurance. For example, in SOC 2 reports, some auditors map controls to HIPAA in an "unattested section 5," but it is important to note this does not provide the same level of assurance as other methods listed above.

On the other hand, HITRUST uses a different approach to assurance called a Validated Assessment Report. This is a comprehensive assessment of an organization's data protection practices and controls conducted by a third-party assessor who has been trained and certified by HITRUST. Once the assessment is complete, HITRUST will issue a Validated Assessment Report detailing the findings of the assessment and may include a certification.

WHY SHOULD I BUY A HIPAA COMPLIANCE ASSESSMENT?

Even though there is no 'formal' HIPAA certification, there are still several reasons why an organization might want to undergo a HIPAA compliance assessment. One reason is to reduce regulatory risk and avoid investigation or litigation with HHS OCR or the states' Attorney Generals. HIPAA requires covered entities to perform a non-technical evaluation of safeguards, and an assessment can help an organization demonstrate it is meeting these requirements. Another reason an organization might get a HIPAA assessment is to honor its ethical obligation to private citizens, whose sensitive information it holds.

WHY SHOULD I BUY A HITRUST ASSESSMENT?

There are several reasons organizations pursue HITRUST Certification. Some of the leading drivers include:

- → Demonstrate commitment to protecting sensitive information: Obtaining HITRUST certification shows your organization is committed to protecting sensitive information and has implemented the necessary controls to do so. This can help build trust with customers and partners.
- → Reduce risk of data breaches: Implementing the controls required for HITRUST certification can help reduce the risk of data breaches and the resulting damage to an organization's reputation and bottom line.
- → Meet customer and vendor requirements: Some customers and vendors may require or prefer an organization be HITRUST certified. Obtaining HITRUST certification can help an organization meet these requirements and maintain its relationships with these stakeholders.

Getting started with HIPAA and HITRUST

If you are new to HIPAA and HITRUST and are looking to protect sensitive health information and comply with best practices, it can be overwhelming to know where to start. Luckily, Thoropass's team of experts can help you navigate these complex frameworks and ensure you select the best one for your organization.