

HIPAA vs HITRUST Info and Link

<https://www.schellman.com/blog/healthcare-compliance/hipaa-vs-hitrust>

What is HIPAA?

An acronym for the Health Insurance Portability and Accountability Act of 1996, HIPAA is a U.S. law that mandates the privacy and security of protected health information (or PHI). It contains three rules applicable organizations must follow regarding Privacy, Security, and Breach Notification.

Such applicable organizations include:

- **Covered Entities:** Healthcare providers, plans, and clearinghouses
- **Business Associates:** Any organization contracted by covered entities or other Business Associates to perform work including ePHI on their behalf

If you fall under this umbrella, you're expected to adhere to the three types of security safeguards:

- Physical
- Technical
- Administrative

That includes complying with the organizational requirements and policies and procedures and documentation requirements. Each of these features a series of standards and specifications to address risks associated with the confidentiality, integrity, and availability of PHI.

HIPAA also includes an evaluation standard that requires periodic technical and nontechnical evaluations to ensure compliance; however, there is no official designation of compliance with HIPAA—rather, you can report their compliance by only providing a completed risk assessment and control documentation.

For those that do not comply, HIPAA is enforced by the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR), which will investigate possible [violations](#) and issue penalties—both financial and otherwise.

What is HITRUST?

While HIPAA is a federal act that sets compliance standards, **HITRUST is an organization that first established its CSF—a security risk and compliance framework—in 2009.** And though HITRUST was initially created to support healthcare industries with specific devotion to the protection of ePHI and PHI, it has since evolved beyond that and can now suit organizations of any industry.

That's because the HITRUST CSF brings together several compliance frameworks, including:

- HIPAA;
- NIST;
- PSI; and
- ISO, as well as some requirements unique to HITRUST.

The HITRUST CSF includes control categories, control objectives, and control specifications. (which may contain multiple levels of control components) spread over multiple Assessment Domains. [To become HITRUST certified, you must meet the appropriate scoring levels for each assessment domain.](#) (This will depend on if you choose an i1 or r2 certification.)

The screenshot shows a blog post from Schellman. The header includes the Schellman logo and navigation links for Services, Industry Solutions, Learning Center, Our Technology, and About Us, along with a yellow 'Contact Us' button. The main content area features a large orange graphic with the title 'HIPAA vs. HITRUST' and icons of a doctor and a shield. Below the graphic, the author is listed as 'By: Schellman' and there is a 'Print/Save as PDF' option. The article title 'HIPAA vs HITRUST' is repeated, followed by the subheading 'HEALTHCARE ASSESSMENTS'. The introductory text reads: 'Consider sugar and salt—both are “spices” of a kind, and since they’re both often in the form of fine white grain, they look similar as well. So similar in fact, you might mistakenly switch one in for the other, setting yourself up for quite the surprise at first bite.' The final line of text is: 'Though not spices, both HIPAA and HITRUST address regulatory compliance for healthcare'.