Lesson 15 | Audits Under HIPAA

Updated 2020-09-12

Audits under HIPAA

Contrary to popular belief and usage, the term “HIPAA Compliant” does not really mean anything. It doesn’t mean anything because it can mean countless things. Did an organization or a product pass a HIPAA audit? And by “pass”, how did the auditor assess the organization or product? An audit is also a point in time. The day after the audit, the organization could change a fundamental thing but the audit would still be a “pass”.

HIPAA does not have approved auditors and does not have an approved certification. As such, many people throw around the term “HIPAA Compliant” without much regard for what it means. This is the reason many covered entities require annual or even quarterly security assessments of all of their partners and vendors.

There have been attempts to fix this. The most popular is HITRUST, which is anchored on a meta-framework that maps to HIPAA, is prescriptive in what it requires, has approved assessors, and issues a true Certification. Some covered entities, especially insurance companies, take HITRUST Certifications in place of their own security assessments.

Whether you do a traditional HIPAA audit or a try for a HITRUST Certification, the most important thing to do is create policies that map to HIPAA (or HITRUST), use those policies to establish procedures for how work should be done, and then document how those procedures are followed across your organization. Having ready access to a body of evidence, your documentation will make any audits and security assessments faster. That alone will also significantly reduce the risk to your organization in the case of a data breach.

Don’t put any stock in the words “HIPAA Compliant”; instead, look for evidence of implementation of policies and procedures.