Safe Harbor Law Benefits Companies That Employ Recognized Security Practices

Your Critical Questions Answered

Covered entities (CEs) and business associates (BAs) that deal with protected health information (PHI) and maintain accredited security standards for more than one (1) year could face lesser fines/penalties and audit scrutiny by the Office for Civil Rights (OCR) in the event of a cyberattack or data breach.

H.R. 7898 – Public Law 116-321, also known as the HIPAA Safe Harbor Law, became law on Jan. 5, 2021.[1] The law's name is a bit of a misnomer, because the exact requirements remain unclear until those are promulgated by the U.S. Department for Health and Human Services (HHS). A better description may be a "protected harbor."

How does the law affect my organization?

Simply put, the law amends the HITECH Act to require HHS to consider "recognized security reports" when considering fines or penalties under the HIPAA Security Rule for CEs and BAs. Fines from the Office of Civil Rights (OCR) can top $1 million, in addition to audit and mitigation costs and loss of business due to adverse publicity.

Obtaining a security accreditation or certification would count as a recognized security practice while providing a high level of assurance for employees, patients, associates and others that data flowing through a company's servers and being exchanged with others is being protected.

EHNAC™

What are 'recognized security practices'?

According to the law, "the term 'recognized security practices' means the standards, guidelines, best practices, methodologies, procedures, and processes developed under section 2(c)(15) of the National Institute of Standards and Technology Act, the approaches promulgated under section 405(d) of the Cybersecurity Act of 2015, and other programs and processes that address cybersecurity and that are developed, recognized, or promulgated through regulations under other statutory authorities. Such practices shall be determined by the covered entity or business associate, consistent with the HIPAA Security rule (part 160 of title 45 Code of Federal Regulations and subparts A and C of part 164 of such title).[2]"

Why is it important?

Cybersecurity remains a critical issue for healthcare providers, payers, clearinghouses, healthcare software vendors, and other covered entities and business associates. According to the OCR Breach Portal, healthcare server breaches were up 23% the first 10 months of 2020 compared to the same period of 2019.[3] Providers accounted for 79% of all healthcare breaches, showing the value of patient information on the black market.[4]

Between January and October 2020, healthcare network server breaches increased 23% over the same 10-month span in 2019. The average cost to mitigate a healthcare data breach tops $7 million, the highest ranked industry and nearly double the global average to mitigate a breach in other industries.

Why EHNAC?

Not all accreditation organizations are created equal. EHNAC is focused only on healthcare, with 20+ accreditation programs specifically designed to safeguard PHI. Each type of healthcare stakeholder has unique needs, and EHNAC programs serve the range of stakeholder types, from health systems to payers to HIEs. EHNAC qualifies as Recognized Security Practices as the NIST cyber-security framework is embedded within its programs. Having been involved with the 405(d) initiative since its inception, EHNAC has served the industry as a federally recognized standards development organization for more than 26 years.

Accreditation may cost less than you think, and certainly a lot less than costs associated with mitigating a breach and potentially paying penalties or fines. EHNAC is a premier accreditation authority promoting standards that support interoperability, stakeholder trust, regulatory compliance, quality service, innovation, and open competition within the healthcare industry.

EHNAC is preparing new "Recognized Security Practices Reports" available to all candidates to specifically demonstrate their compliance with the HIPAA Safe Harbor Law.

[1] https://www.congress.gov/bill/116th-congress/house-bill/7898/text?r=2&s=1

[2] ibid.

[3] https://fortifiedhealthsecurity.com/wp-content/uploads/2020/12/Fortified-Health-Security-2021-Horizon-Report.pdf

[4] https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/

Trust Is Everything in Healthcare

When privacy, security and confidentiality of healthcare data is on the line, a trusted name is a game-changer in today's marketplace. EHNAC accreditation has been trusted and respected in the industry for more than 25 years.

info@ehnac.org | ehnac.org