Bernard Robinson & Company

IT Risk Advisory Services

As Certified Public Accountants and Advisors, BRC is proud to announce our advisory services focused on HIPAA Security and Privacy Risk Assessment.

HIPAA Security and Privacy Risk Assessment Overview

In 2003, the Health Insurance Portability and Accountability Act (HIPAA) introduced the original Privacy Rule, and in 2009 the Health Information Technology for Economic and Clinical Health (HITECH) Act defined policies, procedures, and processes that are required for companies that store, process, or handle electronic protected health information (ePHI). In 2013, the Final Omnibus Rule updated the HIPAA Security Rule and breach notification clauses of the HITECH Act. This rule extended the HIPAA Risk Assessment to "Business Associates".

Every organization (Covered Entity or Business Associate) that creates, receives, maintains, or transmits protected health information (PHI) has to periodically conduct a HIPAA risk assessment in order to comply with §164.308 of the HIPAA Security Rule, even if that PHI is not electronic.

The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) may issue fines for non-compliance to Covered Entities AND Business Associates.

For health information, privacy is defined as the right of an individual to keep his/her individual health information from being disclosed. This is typically achieved through policy and procedure. Privacy encompasses controlling who is authorized to access patient information; and under what conditions patient information may be accessed, used and/or disclosed to a third party. The HIPAA Privacy Rule applies to all protected health information.

Security is defined as the mechanism in place to protect the privacy of health information. This includes the ability to control access to patient information, as well as to safeguard patient information from unauthorized disclosure, alteration, loss or destruction. Security is typically accomplished through operational and technical controls. Since so much PHI is now stored and/or transmitted by computer systems, the HIPAA Security Rule was created to specifically address electronic protected health information.

A HIPAA security assessment evaluates an organization's security and compliance posture against the safeguards specified in the HIPAA Security Rule. It typically consists of interviews, document review and tests of controls. The assessment should be conducted as a risk assessment, but may also consist of a gap assessment against the safeguards specified in the HIPAA Security Rule.

BRC Services for a HIPAA Security and Privacy Assessment

- HIPAA Privacy Compliance Assessment – a review of policies, procedures, testing of privacy controls and interviews with appropriate staff.
- HIPAA Security Assessment – evaluates an organization's security and compliance posture against the safeguards specified in the HIPAA Security Rule.
- Systems Vulnerability Scanning Assessment
- Data Classification Process Design and Consulting

Let's get started today! For more information please contact: Ben Hunter III, CPA, CISA, CRISC, CFE at (336).294.4494 (bhunter@brccpa.com) or any of our dedicated service line leaders.

brccpa.com

Balanced. Responsive. Connected.