Risk Advisory Services

HIPAA Security and Privacy Risk Assessment

As Certified Public Accountants and Advisors, BRC has developed a cybersecurity practice that helps clients stay in compliance with the HIPAA Security and Privacy rules.

Every organization (Covered Entity or Business Associate) that creates, receives, maintains, or transmits protected health information (PHI) must 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.

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's risk advisory team is committed to helping you stay in compliance.

HIPAA Security and Privacy Risk Assessment Services

- **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, CISO, CPA/CITP, CISA, CRISC, CDPSE, CISM at (336).294.4494 (bhunter@brccpa.com) or any of our dedicated service line leaders.

brccpa.com

Bernard Robinson & Company