Consumer Privacy - What You Need To Know

The Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Michelle Merola
Partner, Associate General Counsel
mmerola@hodgsonruss.com
518-736-2917

Gary M. Schober
Partner
gschober@hodgsonruss.com
716-848-1289

Patrick E. Fitzsimmons
Partner
pfitzsim@hodgsonruss.com
716-848-1710

HIPAA was one of the first pieces of legislation in the U.S. to provide a comprehensive approach to data privacy and security. Specifically, this iconic law, and its implementing regulations, establish national standards to safeguard protected health information that is created, received, used, or maintained in an electronic format by a covered entity (ePHI). HIPAA's Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. Thus, it operationalizes the privacy protections contained in HIPAA by addressing the technical and nontechnical safeguards that covered entities must implement to secure ePHI.

For example, the Security Rule requires covered entities to:

- ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;
- identify and protect against reasonably anticipated threats to the security or integrity of the information;
- protect against reasonably anticipated, impermissible uses or disclosures; and
- ensure compliance by their workforce.

The Security Rule does not dictate a one-size fits all approach. Safeguards can be scaled to the size and resources of the covered entity. The following factors should be considered by a covered entity when developing and implementing security measures:

- the size, complexity, and capabilities of the covered entity;
- the technical, hardware, and software infrastructure of the covered entity;
- the costs of the security measures under consideration; and
- the likelihood and possible impact of potential risks to e-PHI.

Under HIPAA, covered entities must constantly review and modify their security measures to continue protecting e-PHI in a changing environment which relies nearly exclusively on electronic records. The importance of HIPAA compliance is underscored by the fact that cyber attacks on healthcare providers have increased exponentially over time.

Hodgson Russ lawyers have deep experience with HIPAA compliance, including HIPAA's technical requirements, security assessments, breach notifications and contractual requirements for business associates. For more information about how Hodgson Russ can assist your organization with HIPAA compliance, email or call one of our Privacy and Security lawyers.