September 19, 2022

NIST Releases Draft Updated Guidance on Implementing the HIPAA Security Rule

On July 21, the National Institute of Standards and Technology (NIST) released draft guidance titled "Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide," NIST Special Publication 800-66, Revision 2 (the Resource Guide), to assist HIPAA-regulated entities of all sizes understand and implement the HIPAA Security Rule. NIST developed the Resource Guide as an update to the HIPAA Security Rule guidance NIST had previously released in 2008; this was as a means of integrating it with other NIST cybersecurity guidance that did not exist when the 2008 guidance was released. Although NIST does not promulgate regulations to enforce HIPAA, the Resource Guide is meant to provide HIPAA-regulated entities with cybersecurity guidance to help maintain the confidentiality, integrity and availability of electronic protected health information (ePHI) in accordance with the HIPAA Security Rule. NIST does not intend the Resource Guide to be a checklist for HIPAA-regulated entities to follow but rather a guide to assist them in managing the risk to ePHI they maintain.

The Resource Guide includes five sections: (1) Introduction; (2) HIPAA Security Rule (sets forth the key concepts of the HIPAA Security Rule); (3) Risk Assessment Guidance (explains the procedure for conducting a risk assessment, the results of which will assist HIPAA-regulated entities in identifying the appropriate security measures to reduce risk to ePHI); (4) Risk Management Guidance (provides a structured process that HIPAA-regulated entities may use to manage identified risks); and (5) Considerations When Implementing the HIPAA Security Rule (highlights key activities that a HIPAA-regulated entity may consider when implementing the HIPAA Security Rule). Section 5 is a particularly helpful resource, as it includes tables organized by each HIPAA Security Rule standard with (1) key activities associated with the security functions suggested by each HIPAA Security Rule standard that a HIPAA-regulated entity may consider implementing; (2) detailed descriptions of the key activities, including an explanation of the relationship between any other relevant HIPAA Security Rule standards; and (3) a non-exhaustive list of sample questions that a HIPAA-regulated entity might ask itself to determine whether a particular HIPAA Security Rule standard has been adequately implemented.

The Resource Guide also includes several additional resources in the appendices, including a crosswalk between the HIPAA Security Rule standards and the NIST Cybersecurity Framework.

NIST is seeking comments on the draft Resource Guide until September 21. For assistance with compliance with the HIPAA Security Rule, please contact William J. Roberts at wroberts@daypitney.com or 860-275-0184 or Stephanie M. Gomes-Ganhão at sgomesganhao@daypitney.com or 860-275-0193.

Would you like to receive our *Day Pitney C.H.A.T. Newsletter?* Sign up here.

Authors

William J. Roberts
Partner

Hartford, CT | (860) 275-0184

wroberts@daypitney.com

Stephanie M. Gomes-Ganhão
Associate

Hartford, CT | (860) 275-0193

sgomesganhao@daypitney.com