Articles + Publications | December 13, 2022

Office of Civil Rights Guidance on Recognized Security Practices Under the 2021 HITECH ?Act Amendment

Privacy & Cybersecurity Newsletter

WRITTEN BY

Laura L. Ferguson

Last year, Congress enacted an amendment to the HITECH Act in January 2021 ("HITECH Amendment") to require that the Department of Health and Human Services ("HHS") consider whether a covered entity or business associate has "adequately demonstrated" it had, for not less than the previous 12 months, "recognized security practices" in place when making certain determinations under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Security Rule (e.g. mitigation of fines, early termination of an audit, or other remedies).[1] The HITECH Amendment provides that "recognized security practices" ("RSPs") include: (i) standards, guidelines, best practices, methodologies, procedures, and processes developed under section 2(c)(15) of the National Institute of Standards and Technology ("NIST") Act; (ii) the approaches promulgated under section 405(d) of the Cybersecurity Act of 2015; and (iii) other programs and processes that address cybersecurity and that are developed, recognized, or promulgated through regulations under other statutory authorities.

On Monday, October 31, 2022, HHS's Office for Civil Rights ("OCR") released a video on RSPs for purposes of the HITECH Amendment. The guidance briefly summarizes OCR's current views on what it means to adequately demonstrate RSPs and answers some questions submitted during the comment period that ended June 2022. The key points from the video include:

- OCR is currently aware of only two RSP standards, both of which are already listed in the statute – NIST Cybersecurity Framework and 405(d) of the Cybersecurity Act of 2015. OCR will publish additional guidance if a regulated covered entity establishes with OCR an RSP standard under the "other" category of the definition under the statute.
- It is insufficient to provide the covered entity's mapping to the NIST Cybersecurity Framework to evidence the implementation of RSPs. OCR wants to see multiple forms of evidence that show the actual implementation, such as:
  - Policies and procedures;
  - Implementation project plan and minutes from meetings;
  - Diagrams and narratives;
  - Training materials;
  - System and application screen shots;
  - Vendor contracts and SOWs related to RSP implementation;
  - Documentation establishing dates of implementation; and
  - Specific examples of implementation of RSPs should be produced. Two examples are: (1) if the RSPs require vulnerability scans, sample results from such scans should be provided; and (2) if the RSPs require mapping data, then the map should be provided.

An entity does not have to produce all of the above. The above is an illustrative list of what is expected from OCR.

- OCR expects to see implementation throughout the entire enterprise – meaning the above evidence should be produced for all servers, workstations, mobile devices, APIs, and other devices/software as applicable to the RSPs. OCR stressed the importance of maintaining an accurate inventory of all IT assets (hardware and software) and noted that both NIST and 405(d) would require this.
- Proving RSPs to OCR is **not** considered to be a safe harbor for compliance with the Security Rule. Regulated entities are not immune from liability for Security Rule violations if they implement RSPs. Implementing RSPs is voluntary and is solely being used by OCR to encourage entities to implement RSPs.Implementation may mitigate penalties/fines/enforcement action if OCR audits an entity and determines there are deficiencies.

Many covered entities and business associates are already utilizing the NIST Cybersecurity Framework or Section 405(d) of the Cybersecurity Act of 2015 to address the requirements of the HIPAA Security Rule, but they may not have documentation readily available to prove up the enterprise-wide implementation of such RSPs. We recommend conducting (or updating) an IT asset inventory and, to the extent feasible for an entity, documenting the system-wide implementation of RSPs in order to prepare the entity to respond to OCR in the event of a security incident that triggers an audit or investigation.

***

[1] The HITECH amendment is available at: https://www.congress.gov/116/plaws/publ321/PLAW-116publ321.pdf.

RELATED INDUSTRIES + PRACTICES

- Health Care + Life Sciences
- Privacy + Cyber