Health Information Compliance Alert

Policy: Feds Invite Feedback on HIPAA and HITECH Provisions

RFI focuses on aspects of HIPAA security and compensation after breach.

Designing and implementing a plan to address your data security risks is an important part of the HIPAA Security Rule requirements. However, the feds may want you to go a step further and detail the "how" of your compliance program execution, a new Request for Information (RFI) suggests.

The HHS Office for Civil Rights (OCR) wants to know what you think about two critical provisions concerning HIPAA and HITECH, according to an RFI published in the Federal Register on April 6. "This Request for Information has long been anticipated, and we look forward to reviewing the input we receive from the public and regulated industry alike on these important topics," said OCR Director **Lisa J. Pino** in a release. "I encourage those who have been historically underserved, marginalized, or subject to discrimination or systemic disadvantage to comment on this RFI, so we hear your voice and fully consider your interests in future rulemaking and guidance."

Read on for a breakdown.

Know These Details on Part 1 of the RFI

The first part of the RFI deals with a HIPAA safe harbor referenced in an amendment to HITECH that was enacted in January 2021 (see Health Information Compliance Alert, Vol. 21, No. 9). Covered entities (CEs) and their business associates (BAs) need to "adequately demonstrate" that they implemented "recognized security practices" 12 months prior to a breach, the amendment indicates.

The RFI goes beyond that initial change and asks for stakeholder feedback on how CEs and BAs are putting their security policies into daily practice. "The RFI solicits comments on how covered entities and business associates understand and are implementing recognized security practices, how they anticipate adequately demonstrating security practices are in place, and other implementation issues they are considering or would like OCR to clarify for the public," says attorney **Igor Gorlach** with King & Spalding LLP in the firm's Health Headlines blog.

Gorlach adds, "OCR notes that it expects 'adequate demonstration' to include the implementation and not merely adoption of the practices."

Caveat: The HITECH amendment outlines "recognized security practices" as "standards, guidelines, best practices, methodologies, procedures, and processes developed under section 2(c)(15) of the National Institute of Standards and Technology Act" and "the approaches promulgated under section 405(d) of the Cybersecurity Act of 2015" while offering a timeline. However, "the HITECH Act does not state what action initiates the beginning of the 12-month lookback period," caution attorneys **Jennifer J. Hennessy, Jennifer L. Urban,** and **Tiffany T. Young** with law firm Foley & Lardner LLP in online analysis.

"It is unlikely that an entity's security plan quickly rolled out upon receiving an HHS investigative letter subsequent to a data incident or complaint will meet the required look-back period," Hennessy, Urban, and Young explain. "Entities should therefore determine if their security practices meet the thresholds in the HITCH Act for 'recognized security practices' and if not, swiftly move to bring those security practices into conformance to start the clock ticking on the 12-month look-back period."

Bonus: Weighing in on the RFI offers CEs and BAs a chance to impact OCR's future rulemaking on the safe harbor, says Wyrick Robbins Yates & Ponton LLP in a post from the law firm's Practical Privacy blog. "The practical benefits could include greater clarity on what OCR expects when it comes to compliance with the HIPAA Security Rule, and a more detailed roadmap for organizations seeking to meet those expectations," Wyrick Robbins attorneys observe.

Understand These Fundamentals on the Second Half of the RFI

Another part OCR's request concerns whether civil money penalties (CMPs) garnered from settlements should be shared with harmed individuals. "Section 13410(c)(3) of the HITECH Act requires the Secretary to establish a methodology for the distribution of a percentage of a CMP or monetary settlement amount collected for noncompliance with the HIPAA Rules to an individual harmed by the noncompliance," the RFI explains.

However, one of the problems with the statute is that it "does not define 'harm,' nor does it provide direction to aid HHS in defining the term," OCR acknowledges.

"This RFI solicits public comment on the types of harms that should be considered in the distribution of CMPs and monetary settlements to harmed individuals and the suitability of the described potential methodologies for sharing and distributing monies to harmed individuals, and invites the public to submit any alternative methodologies that are not identified herein," OCR states.

Deadline: OCR will accept public comments through June 6. You can read the RFI and comment in the Federal Register at www.federalregister.gov/documents/2022/04/06/2022-07210/considerations-for-implementing-the-health-information-technology-for-economic-and-clinical-health.