akerman

Blog Post

Help Wanted: OCR Seeks Public Input on "Recognized Security Practices" and Sharing Settlements with Harmed Individuals Under the HITECH Act

April 18, 2022
By Elizabeth F. Hodge

Covered entities and business associates subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) have the chance to provide input on two amendments to the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act). The U.S. Department of Health and Human Services Office for Civil Rights (OCR) recently issued a Request for Information (RFI) seeking public input regarding:

1. How covered entities and business associates (collectively, regulated entities) are voluntarily implementing "recognized security practices" as identified in the HITECH Act and demonstrating how such practices are in use throughout the organization.
2. The types of harms that should be considered in distributing civil monetary penalties (CMPs) and monetary settlements to harmed individuals and potential methodologies for sharing and distributing CMPs and settlement funds to harmed individuals.

We discuss the two topics covered in the RFI in more detail below.

Related People

Elizabeth F. Hodge

Related Work

Healthcare
Healthcare Licensure and Compliance

Related Offices

West Palm Beach

Health Law Rx

Akerman Perspectives on the Latest Developments in Healthcare Law

Visit this Akerman blog

Recognized Security Practices

The HITECH Act was amended effective January 5, 2021 (Amendment) to require that HHS consider whether a regulated entity has adequately demonstrated that it had in place for at least the previous twelve months "recognized security practices." The existence of those recognized security practices may mitigate potential fines, result in early termination of audit activities, and mitigate other remedies that might be agreed to in resolving potential violations of the HIPAA Security Rule following an investigation, compliance review, or audit. The goal of the Amendment is to encourage regulated entities to do "everything in their power to safeguard patient data."

The Amendment defines "recognized security practices" as:

- the standards, guidelines, best practices, methodologies, procedures, and processes developed under section 2(c)(15) of the National Institute of Standards and Technology (NIST) Act;
- the approaches promulgated under section 405(d) of the Cybersecurity Act of 2015; and
- other programs and processes that address cybersecurity and that are developed, recognized, or promulgated through regulations under other statutory authorities.

Notably, the HITECH Act does not *require* regulated entities to implement recognized security practices, nor does it specify how regulated entities should select which category of recognized security practices to implement. However, to be considered for mitigation of fines and other remedial requirements, organizations must be able to demonstrate that they have fully implemented the recognized security practices for the preceding twelve months. Simply providing initial documentation of the adoption of the security practices is insufficient. Rather, the regulated entity must demonstrate that such practices and

procedures have been in continuous operation for at least twelve months. The statute does not specify what triggers the beginning of the twelve-month look-back period.

The RFI requests that regulated entities provide input to OCR regarding their voluntary implementation of recognized security practices, including addressing the following questions:

- What recognized security practices have regulated entities implemented and what recognized security practices do regulated entities plan to implement?
- What standards, guidelines, and procedures developed under section 2(c)(15) of the NIST Act do regulated entities rely on when establishing and implementing recognized security practices?
- What approaches promulgated under section 405(d) of the Cybersecurity Act of 2015 do regulated entities rely on when establishing and implementing recognized security practices?
- What other programs and processes that address cybersecurity (besides those developed under section 2(c)(15) of the NIST Act or section 405(d) of the Cybersecurity Act of 2015) and that are developed, recognized, or promulgated through regulations under other statutory authorities do regulated entities rely on when establishing and implementing recognized security practices?
- What steps do covered entities take to ensure that recognized security practices are in place?
- What steps do covered entities take to ensure that recognized security practices are in use throughout their enterprise and what constitutes implementation throughout the enterprise?
- What steps do covered entities take to ensure that recognized security practices are actively and consistently in use continuously over a 12-month period?

Notably, in the RFI OCR refers to “regulated entities” in the first four questions and “covered entities” in the last three questions above. Based on the full text of the RFI, it is unclear why OCR appears to limit the last three requests to covered entities and exclude business associates.

Sharing Civil Monetary Penalties and Settlements with Individuals

The HITECH Act also requires HHS to establish by regulation a methodology under which an individual harmed by a potential violation of the HIPAA Privacy, Security, and/or Breach Notification Rules may receive a percentage of any civil monetary penalty or monetary settlement collected with respect to such offense. The methodology must be based on recommendations submitted by the General Accounting Office (GAO). OCR must base its determinations of appropriate penalty amounts on the nature and extent of the violation and the nature and extent of the harm resulting from the violation. Under the HIPAA Enforcement Rule, OCR may consider physical harm, financial harm, reputational harm, and harms that hinder one’s ability to obtain health care as aggravating factors in assessing a CMP or proposed settlement amount. However, the HITECH Act does not define “harm” generally nor the specific types of harm that OCR may consider in assessing CMPs or settlement amounts. How OCR ultimately defines what constitutes compensable harm could have far-reaching consequences beyond enforcement of HIPAA.

The GAO has recommended that OCR consider three models for the methodology to distribute a portion of CMPs and settlement amounts to individuals:

- The Individualized Determination Model, where the plaintiff bears the burden of proof with respect to the harm suffered by the plaintiff and the liability incurred by the defendant;
- The Fixed Recovery Model, where awards are either fixed or calculated by a formula established

by law; and

- The Hybrid Model, which combines elements of the Individualized Determination Model and the Fixed Recovery Model.

To assist it in evaluating the methodologies recommended by the GAO, OCR seeks input from all stakeholders regarding:

- How to define "harm," including what constitutes compensable harm for violations of HIPAA and whether harm should include non-economic harms such as emotional harm;
- What bases should be used for deciding which injuries are compensable;
- What factors should be considered in establishing a methodology for calculating the amount to be set aside for distribution to individuals;
- Whether there are circumstances in which funds should not be set aside for distribution to individuals; and
- How to provide notice to affected individuals that monetary distribution may be available.

HIPAA covered entities, business associates, and other stakeholders that want to respond to one or both topics in the RFI must submit comments to OCR by June 6, 2022. While OCR assesses how it will respond to comments, covered entities and business associates should consider: (i) implementing recognized security practices; and (ii) how they will document that such practices are in continuous use throughout the organization to avail themselves of the mitigation afforded by the Amendment. Covered entities and business associates should consult healthcare attorneys for assistance in this analysis.

Update should be construed as legal advice or a legal opinion, and readers should not act upon the information contained in this Practice Update without seeking the advice of legal counsel. Prior results do not guarantee a similar outcome.