PUBLICATION

Office For Civil Rights Seeks Input on Implementation of HITECH Amendments

Authors: Layna S. Cook Rush
April 08, 2022

On April 6, 2022, the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) released a Request for Information (RFI) seeking public comment on "recognized security practices" and on sharing civil monetary penalties and monetary settlements under the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act). The HITECH Act was amended on January 5, 2021. The amendment requires HHS to consider certain recognized security practices of covered entities and business associates when making determinations on whether to impose penalties for violation of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Covered entities and business associates are not required to implement recognized security practices, but if they can demonstrate recognized security practices are in place for a 12-month period before an incident, those practices will be considered as a mitigating factor in the analysis of a penalty for violation of HIPAA.

Recognized security practices are defined as the standards, guidelines, best practices, methodologies, procedures and processes developed under any of the following:

- section 2(c)(15) of the National Institute of Standards and Technology (NIST) Act;
- section 405(d) of the Cybersecurity Act of 2015; or
- other programs and processes that address cybersecurity and that are developed, recognized, or promulgated pursuant to other statutory authorities.

The recent RFI seeks comment on how covered entities and business associates:

- understand and are implementing recognized security practices;
- anticipate adequately demonstrating that recognized security practices are in place; and
- implementation issues that they would like OCR to clarify for the public and stakeholders through potential guidance or rule making.

OCR's specific questions with regard to implementation of recognized security practices include:

- What recognized security practices have regulated entities implemented?
- What standards, guidelines, best practices, methodologies, procedures and processes have been developed under NIST, the Cybersecurity Act of 2015 or other statutory authorities?
- 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 used throughout their 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?

The amendments to the HITECH Act also require HHS to establish a methodology under which individuals harmed by potential violation of HIPAA can receive a percentage of any civil monetary penalty or monetary settlement collected for the offense. OCR is seeking input from commentators on how to define harm that would warrant compensation and how compensation should be determined.

OCR is seeking comment from all stakeholders including patients and their families, HIPAA covered entities and business associates, consumer advocates, health information technology vendors and government entities. Comments must be submitted by June 6, 2022 in order to be considered.

For more information, contact Layna Cook Rush, CIPP/US, CIPP/C or your Baker Donelson Health Law attorney.