White and Williams LLP

HITECH Act Amendment Offers New Incentive to Reduce Fines and Other Remedies

By: Joshua A. Mooney, Debra A. Weinrich and Linda D. Perkins
Cyber Law and Data Protection and Healthcare Alert
1.8.21

Just in case your office or company is in the process of compiling a "to-do" list for 2021, here is one item that should have your full attention. On January 5, 2021, an amendment to the HITECH Act (H.R.7898) was signed into law requiring the U.S. Department of Health and Human Services "to consider certain recognized security practices of covered entities and business associates when making certain determinations, and for other purposes." While the amendment does not include specific language as to what "consider" may mean in this context, Section 13412(a) makes clear the incentives for covered entities having "certain recognized security practices," namely:

> [T]he Secretary shall consider whether the covered entity or business associate has adequately demonstrated that it had, for not less than the previous 12 months, recognized security practices in place that may—
>
> (1) mitigate fines under section 1176 of the Social Security Act[];
>
> (2) result in the early, favorable termination of an audit under section 13411; and
>
> (3) mitigate the remedies that would otherwise be agreed to in any agreement with respect to resolving violations of the HIPAA Security rule . . . between the covered entity or business associate and the Department of Health and Human Services.

Section 13412(b) defines the term "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." In addition, "[s]uch practices shall be determined by the covered entity or business associate, consistent with the HIPAA Security rule[.]"

The amendment expressly states that "[n]othing in this section shall be construed as providing the Secretary authority to increase fines . . . or the length, extent or quantity of audits under section 13411, due to a lack of compliance with the recognized security practices." Finally, the amendment provides that "nothing in this section shall be construed to subject a covered entity or business associate to liability for electing not to engage in the recognized security practices defined by this section[.]"

In other words, this new law offers significant incentives for simply being able to demonstrate to some unspecified degree the existence of recognized security practices. The amendment does not require or impose a standard for compliance with those security practices and leaves it to the covered entity or business associate to determine what those "recognized security practices" are for their particular operation.

The members of our Healthcare Industry Team and Cyber Law and Data Protection Group are available to discuss with you any questions you may have about how to make sure your business or company can benefit from Section 13412 should it face a compliance audit or review in the future. For additional information or if you have any questions, please contact Debra A. Weinrich (weinrichd@whiteandwilliams.com; 215.864.6260) or Linda D. Perkins (perkinsl@whiteandwilliams.com; 215.864.6866).