HIPAA's Next Act

Client Alert
6.1.2022

The Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services issued a Request for Information (RFI) seeking input from the public on how the healthcare industry understands and implements "recognized security practices." The RFI also seeks input on how individuals harmed by HIPAA violations should be compensated. Comments are due by June 6, 2022. The implementation of changes arising out of the RFI could be a game changer for Covered Entities and Business Associates.

RECOGNIZED SECURITY PRACTICES

So, what is a "recognized security practice?" When determining the fines to be assessed in the event of a breach, HHS will consider those recognized security practices that have been in place for 12 months. The determination of what is a "recognized security practice" is very important. Also critical is when does the 12 month period start to run. Therefore, the RFI is seeking input on what are the recognized security practices that are in common use. One of the dangers here for both Covered Entities and Business Associates alike is that the results of the RFI will come from input by larger health care providers and others who have larger budgets for security and so rather than have a "scalable" approach as was intended, a more restrictive standard of what is a "recognized security practice" is adopted.

The concept for implementation of "recognized security practices" and HHS's consideration of the same was enacted on January 5, 2021 through an Amendment to the Health Information Technology for Economic and Clinical Health 42 USC P.L. 116-321 ("HITECH Act") Act, which mitigates fines and penalties for a HIPAA breach if the affected Covered Entity or Business Associate could demonstrate it had such "recognized security practices" in place at least 12 months prior to the breach investigation of audit. The Amendment defines "recognized

Related People

Debra A. Geroux
Shareholder

Robert H. Schwartz
Shareholder

Related Services

Health Care

Health Care Industry Team

HIPAA

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 Act, the approaches promulgated under Section 405(d) of the Cybersecurity Act of 2015; and other programs and processes that address cybersecurity that are developed, recognized, or promulgated through regulations under other statutory authorities. Since its enactment, OCR has been requesting documentation of Covered Entities' and Business Associates' security practices as part of its investigation into reported Breaches, without providing guidance as to what, specifically, they are considering. However, the RFI points out that OCR's position is that it is insufficient for a regulated entity to just establish and document the adoption of recognized security practices. OCR requires that the entity fully implement and actively and consistently use the recognized security practices. OCR will take these actions into account in an audit or investigation, when determining what, if any, mitigation will be acceptable. One of the benefits of the RFI is that it does provide Covered Entities and Business Associates a checklist of what can be used in defense of an OCR breach investigation.

COMPENSATION OF INDIVIDUALS

Since its inception, HIPAA has not provided for any private cause of actions for individuals affected by a Breach of their protected health information, although OCR does recognize that HIPAA does not preclude remedies under state or other law. In the RFI, HHS is seeking information regarding compensation of individuals harmed by HIPAA violations. The Secretary is considering the establishment of rules whereby individuals may receive a percentage of civil monetary penalties ("CMP") or a percentage of a monetary settlement actually collected. The HIPAA enforcement rule had previously identified 4 types of harm: physical, financial, reputational, and harms that hinder one's ability to obtain healthcare. The RFI is seeking information on what types of harm should be compensable for HIPAA violations and an appropriate methodology that should be adopted to facilitate monetary awards.

Among the questions OCR is asking regarding potential compensation are:

1. Are there any circumstances in which harms should be presumed?
2. Does harm include the release of information about a person other than the individual that is the subject of the information?
3. Should OCR implement a minimum or maximum limit for the total amount of any penalty a harmed individual may be compensated for?
4. What constitutes compensable harm?
5. Should compensable harm be limited to past harm?
6. Should only economic harm be considered?
7. Should harm be limited to the types of harms identified as aggravating factors in assessing CMPs?
8. Should harm be expanded to include additional types of noneconomic harms such as emotional harm?

9. How should harmed individuals be identified? How should they be notified? What if they are deceased? What if they cannot be located? What is the period of time for claims to be made?
10. What methodologies should OCR consider for sharing and distributing monies to harmed individuals? Should there be a minimum or maximum amount or percentage? Should there be an appeals process?

OCR is reviewing several different compensation models for compensating individuals harmed by HIPAA violations. The Model identified in the RFI are: (i) the Individualized Determination Model; (ii) the Fixed Recovery Model and (iii) the Hybrid Model. OCR is soliciting input to determine which model stakeholders believed would work best. OCR based the Individualized Determination Model on the private civil claims model. In this model, the burden is on the individual to prove that he/she was damaged and to what extent, and the thinking is that each claim would need to be heard by a jury. This approach would be similar to that used for the Consumer Financial Protection Bureau. The Fixed Recovery Model would award victims a set amount based on a fixed formula, similar to the current Black Lung Benefits Act model. The Hybrid Model combines elements of the other 2 models and sets a minimum award with additional compensation for those individuals that can prove that a higher award is warranted.

As noted above, HIPAA violations may be subject to state or other law for which no preclusion would apply. With such a statement, it begs the question of whether OCR is inviting the plaintiff's bar to bring more actions involving a Covered Entity or Business Associate's failure to follow the requirements of HIPAA. One of the implications of the RFI is to possibly promote class actions as a framework for HIPAA violations, which is a concept that has been occurring with varying results for years. Another outcome of OCR's statement is the possibility of enticing more whistleblowers to come forward by dangling larger awards in front of them.

While comments to the RFI are due June 6, 2022, the final rules or guidance will not be immediately forthcoming. We encourage our readers watch for further developments in this area as the landscape may be radically changing. The next act of HIPAA may force greater compliance, but it may also force those who are responsible for privacy and security to be less forthcoming about issues that they have to address. As we learn more, we will bring the developments to your attention. In addition to the authors, members of Butzel's Health Care Industry Team would be pleased to answer any questions you may have about this client alert or any other related matter.

Debra Geroux
248.258.2603
geroux@butzel.com

Mark Lezotte
313.225.7058
lezotte@butzel.com

CLIENT ALERTS

Robert Schwartz
248.258.2611
schwartzrh@butzel.com