Codify
BY AAPC

Health Information Compliance Alert

HITECH: RFI Spells Trouble for Breached Practices in the Future

Feds look at ways to quantify HIPAA breaches - and pay patients for lost PHI.

Though statistics suggest large-scale HIPAA breaches are on the decline, even a small problem can come at a cost - both personal and financial. However, the Department of Health and Human Services (HHS) wants to delve more deeply into that cost and, possibly, put a price tag on the human trauma of lost protected health information (PHI).

Context: Back in 2009, the Health Information Technology for Economic and Clinical Health (HITECH) Act was established to promote and govern health IT, which at that time was still an evolving market. As the years have passed, many of the policies outlined in the HITECH Act have come to fruition and been implemented. However, one subpart that falls under Section 13410 and covers one aspect of HIPAA has fallen by the wayside, even though it was required for ramp-up in 2012 - until now.

Many are familiar with HITECH's Section 13410, Subtitle D as it looks specifically at the four penalty tiers for civil monetary penalties (CMPs) for HIPAA violations. It discusses the way these violations are determined and paid out through "increasing levels of culpability," according to the HHS Office for Civil Rights (OCR) summary (See Health Information Compliance Alert, Vol. 19, No. 7 for more information on the tiers).

You can read the OCR breakdown of Section 13410, Subtitle D at www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html.

New: But, according to an advanced notice of proposed rulemaking (ANPRM) that would solicit a request for information (RFI) from the public, the feds want to home in on how CMPs are distributed - to patients.

In the past, covered entities (CEs) paid fines to the government for HIPAA breaches with the maximum penalty at $1.5 million, which is now adjusted to $1,650,300 for inflation. HITECH requires, however, that HHS come up with an add-on formula that forces CEs to make amends financially with patients whose PHI has been compromised.

"HHS plans to issue a request for information [RFI] on a proposal to share a percentage of money paid by healthcare organizations through civil monetary penalties or monetary settlements resulting from data breaches with the affected individuals," writes attorney **Sarah Beth S. Kuyers** with the national law firm **Mintz, Levin, Cohn, Ferris, Glovsky, and Popeo, PC** in analysis of the proposal in the Mintz Insights blog. "The request was supposed to be issued in November but has been pushed to January."

Here's What's on the Table

Subtitle C of Section 13410 of HITECH looks specifically at figuring out how to financially calculate the loss of PHI or electronic PHI (ePHI). This is a big issue for providers, warns **Jim Sheldon-Dean**, founder and director of compliance services at **Lewis Creek Systems LLC** in Charlotte, Vermont.

"This has more pitfalls and issues than anything HHS has had to come up with in a long time," maintains Sheldon-Dean. "The regulatory burden is significant."

Specifics: In a Government Accountability Office (GAO) report, the feds suggest that harmed individuals "may receive a percentage of any civil monetary penalty or monetary settlement collected with respect to such offense," outlines Section 13410 (c)(2) of HITECH. HHS wants to study that order in its RFI, which is better explained in the following Subtitles, which define the methodology reasoning. Take a look at HITECH Section 13410, Subtitles (c)(3) and (c)(4):

- **Subtitle 3: Establish a formula.** "Not later than 3 years after the date of the enactment of this title, the

Secretary shall establish by regulation and based on the recommendations submitted under paragraph (2), a methodology under which an individual who is harmed by an act that constitutes an offense referred to in paragraph (1) may receive a percentage of any civil monetary penalty or monetary settlement collected with respect to such offense," the HITECH Act says.

- **Subtitle 4: Implement the plan.** "The methodology under paragraph (3) shall be applied with respect to civil monetary penalties or monetary settlements imposed on or after the effective date of the regulation," indicates the HITECH Act.

Consider This Expert Input

CEs have been worried about this section since HITECH's inception, and experts agree they have reason to be concerned. "There is currently no clear methodology for determining when an individual is harmed by a data breach and how much money any one individual would deserve for the resulting harm," says Kuyars.

She cautions, "This determination would be particularly difficult for large data breaches involving hundreds, if not thousands, of unspecified victims whose information may have been left vulnerable but not actually exploited."

Important: Sheldon-Dean agrees. "How do you define harm?" he asks. "What if some people are harmed more than others?" He wonders, too, how "will a payout in the tens of dollars satisfy anyone in the case of a large breach where the maximum penalties are to be shared among tens of thousands of individuals?"

Since every HIPAA breach is different, it's tough to imagine that a one-size-fits-all formula for patient compensation will work. The RFI aims to help HHS determine CEs' thoughts on the layout of a methodology, but the agency has not communicated the logistics of implementing such a complicated plan.

Money matters: Whether the feds finalize a policy and roll out this HIPAA regulatory reform in 2019 or the years ahead, they've banked a substantial amount of CMP funds from past HIPAA indiscretions. "HHS has collected almost $40 million since it began imposing civil monetary penalties, a considerable sum that could be distributed to affected individuals," notes online analysis of the ANPRM by national law firm **Hunton Andrews Kurth LLP** in its Privacy and Information Security Law Blog.

Note: See the advanced ANPRM at www.reginfo.gov/public/do/eAgendaViewRule?pubId=201810&RIN=0945-AA04.