Health Information Compliance Alert

HIPAA: Do CMP Rollbacks Signal Major Changes for HIPAA Enforcement?

Hint: Risk management is even more important now.

After producing record-level HIPAA enforcement numbers last year, the feds shocked many last month with new Civil Monetary Penalty (CMP) guidance. In an about-face turnaround the feds announced that they were drastically reducing penalty caps for HIPAA violations - active immediately.

Background: The Department of Health and Human Services (HHS) published the "Notification of Enforcement Discretion Regarding HIPAA Civil Money Penalties" in the Federal Register on April 30. Acting on HITECH Act provisions, HHS determined that current CMP caps for HIPAA violations do not differentiate accordingly with the levels of culpability under the four Tiers, indicates the release.

Under the current HIPAA Enforcement Rule, HHS "applies an annual upper limit of $1.5 million for each of the four culpability Tiers," reminds the notice. However, that kind of one-fine-fits-all methodology doesn't seem fair and contributes to the feds' reasoning. "HHS modified this approach and will now apply a different annual cap to each Tier, thus making the Tiers more meaningful and softening the financial impact of HIPAA violations that fall into the lower Tiers," explain attorneys **H. Carol Saul** and **Madison M. Pool** in the Atlanta office of **Arnall Golden Gregory LLP,** in online analysis of the notice.

Here Are the Details

According to HHS, CMP caps needed to be updated to align with culpability levels outlined in the HITECH Act. In simple terms, it didn't seem fair that a covered entity (CE) who unknowingly committed a basic HIPAA violation (Tier 1) should have the same annual limit and financial accountability as a CE who willfully neglected to correct actions that led to a HIPAA violation (Tier 4).

"While most of the annual maximums have been reduced, the concept of tying the penalty to the level of culpability has been in the law all along, and the former $1.5 million annual limit for any type violation didn't reflect that," says **Jim Sheldon-Dean**, founder and director of compliance services for **Lewis Creek Systems, LLC** in Charlotte, Vermont. "But keep in mind that the maximums are for any one violation type, and in an incident, there are usually several rules at play, so the maximums can easily be multiplied."

Take a look at an overview of the CMP cap changes:

New Limits May Translate to More Compliance Planning Scrutiny

The reduced limits are sure to come as a relief to providers worried about the financial aftershocks of a breach, but experts warn that practices aren't off the HIPAA compliance hook. In fact, the changes signal to many that the **HHS Office for Civil Rights** (OCR) is placing more importance on following through on risk management than ever before. And CEs racking up violations must prepare themselves for heightened scrutiny of their compliance planning.

"If an organization does not do a sufficient job of addressing the rules, an incomplete compliance effort, such as ignoring repeated recommendations to reduce risks, can easily be seen as a more culpable situation," Sheldon-Dean warns. This puts "the entity into a higher penalty bracket, and the new distinction between penalty levels may provide a greater opportunity for HHS to reasonably use the 'willful neglect' levels of penalty."

That's why it may be more fiscally savvy to put your money into risk assessment and analysis upfront instead of after the fact.

Tip: "The costs of non-compliance are usually far greater than the costs of compliance with HIPAA - the rules are, for the most part, common-sense based," says Sheldon-Dean. And, he reminds practices not to forget about inflation when calculating annual limits.

"Also, keep in mind that all of the penalty levels have had their numbers adjusted by a roughly 14 percent cost-of-living adjustment, so that the $1.5 million maximum for a Tier 4 penalty is now $1,711,533," explains Sheldon-Dean

Bottom line: For the past 13 years, **IBM** and the **Ponemon Institute** have published an annual "Cost of a Data Breach Study," and as the risks have increased, so have the costs. Last year's results concluded that "the global average cost of a data breach is up 6.4 percent over the previous year to $3.86 million," notes the IBM and Ponemon Institute study. "The average cost for each lost or stolen record containing sensitive and confidential information also increased by 4.8 percent year over year to $148." The 2019 report is expected sometime this summer.

Resource: Review the "Notification of Enforcement Discretion Regarding HIPAA Civil Money Penalties" at www.govinfo.gov/content/pkg/FR-2019-04-30/pdf/2019-08530.pdf.