HHS Issues "Enforcement Discretion" Notice Concerning HIPAA Penalties

HHS Issues "Enforcement Discretion" Notice Concerning HIPAA Penalties

On April 30, 2019, the U.S. Department of Health & Human Services (HHS) issued a Notice of Enforcement Discretion in the Federal Register (Notice) to inform the public about how it applies HHS regulations concerning the assessment of civil monetary penalties (CMPs) for HIPAA violations.

Both civil and criminal penalties are possible under HIPAA. Civil monetary penalties are tiered across four categories based on the violation type: (1) the person did not know (and, by exercising reasonable diligence, would not have known) that the person violated the provision of HIPAA at issue, (2) the violation was due to reasonable cause, and not willful neglect, (3) the violation was due to willful neglect that is timely corrected, and (4) the violation was due to willful neglect that is not timely corrected. In publishing the HIPAA Enforcement Rule in 2013, HHS interpreted HIPAA's statutory language to apply civil monetary penalties in the following manner:

Culpability	Min. Penalty/Violation	Max. Penalty/Violation	Annual Limit Identical Violations
No Knowledge	$100	$50,000	$1,500,000
Reasonable Cause	$1,000	$50,000	$1,500,000
Willful Neglect – Corrected	$10,000	$50,000	$1,500,000
Willful Neglect – Not Corrected	$50,000	$50,000	$1,500,000

The fourth column indicates the annual limit for all violations of an identical requirement or prohibition. In commentary to the 2013 HIPAA Enforcement Rule, HHS noted that some commenters expressed concern about the $1.5 million cap for every penalty tier, and that this was inconsistent with the HITECH Act. At the time, HHS stated that it continued to believe the penalty amounts were appropriate and reflected "the most logical reading of the HITECH Act."

In the Notice, HHS stated that, upon further review, "the better reading" of the HITECH Act is to apply the annual limits as follows:

Culpability	Min. Penalty/Violation	Max. Penalty/Violation	Annual Limit Identical Violations
No Knowledge	$100	$50,000	$25,000
Reasonable Cause	$1,000	$50,000	$100,000
Willful Neglect – Corrected	$10,000	$50,000	$250,000
Willful Neglect – Not Corrected	$50,000	$50,000	$1,500,000

HHS advised that it will use the above civil money penalty structure, as adjusted for inflation, effective as of the date of the Notice and until further notice. HHS also commented that it "expects to engage in future rulemaking to revise the penalty tiers in the current regulation to better reflect the text of the HITECH Act."

It will be interesting to watch HHS's implementation of the revised annual limit interpretation and whether some of the shocking penalties of the past couple of years will continue to be seen, e.g., a $5.5 million penalty assessed against Memorial Healthcare System in 2017 and a $16 million penalty assessed against Anthem in 2018. Perhaps HHS will issue more violations in each case it reviews to make up the difference. Perhaps HHS will issue more lower-end penalties in lieu of its determination to provide "technical assistance" rather than a penalty in certain cases.

For now, we will have to wait and see whether covered entities and business associates will benefit from the HHS's updated interpretation of the tiered penalty structure. What we do know for sure is that willfully neglectful behavior will result in maximum penalties. This type of behavior may include not having up-to-date policies in place, not having business associate agreements in place where needed, and not performing periodic risk analyses and/or addressing identified risks and vulnerabilities.

For more information or assistance with your organization's HIPAA privacy and security program or a breach incident, contact:

Lani M. Dornfeld, CHPC | 973.403.3136 | ldornfeld@bracheichler.com