Billing Code: 4153-01-P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

45 CFR Part 160

Notification of Enforcement Discretion Regarding HIPAA Civil Money Penalties

AGENCY: Office of the Secretary, HHS.

ACTION: **Enforcement Discretion.**

SUMMARY: This notification is to inform the public that the Department of Health and Human Services (HHS) is exercising its discretion in how it applies HHS regulations concerning the assessment of Civil Money Penalties (CMPs) under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as such provision was amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act. Current HHS regulations apply the same cumulative annual CMP limit across four categories of violations based on the level of culpability. As a matter of enforcement discretion, and pending further rulemaking, HHS will apply a different cumulative annual CMP limit for each of the four penalties tiers in the HITECH Act.

DATES: This exercise of enforcement discretion is effective indefinitely.

FOR FURTHER INFORMATION CONTACT: Rachel Seeger at (202) 619-0403 or (800) 537–7697 (TDD).

SUPPLEMENTARY INFORMATION:

I. Background

When enacting the HIPAA administrative simplification provisions, Congress authorized HHS to impose a maximum CMP of $100 for each violation, subject to a calendar year cap of $25,000 for all violations of an identical requirement or prohibition. Pub. L. 104-191, section

262(a), 110 Stat. 1936, 2028 (Aug. 21, 1996) (adding Social Security Act section 1176(a)(1), 42 U.S.C. 1320d-5(a)(1)).

HHS issued an interim final rule (IFR) on April 17, 2003, setting forth the procedural requirements that the Department would follow in enforcing HIPAA and its regulations, including procedures for providing notice, managing hearings, and issuing administrative subpoenas. HHS issued a proposed rule on the substantive enforcement provisions on April 18, 2005. HIPAA Administrative Simplification: Enforcement; Proposed Rule, 70 FR 20224 (April 18, 2005). HHS issued a HIPAA enforcement final rule on February 16, 2006, which, among other things, incorporated penalties consistent with the $100 per violation cap and $25,000 annual cap in HIPAA. HIPAA Administrative Simplification: Enforcement; Final Rule, 71 FR 8390 (Feb. 16, 2006).

In February 2009, Congress enacted the HITECH Act (as part of the American Recovery and Reinvestment Act of 2009) that, among other things, strengthened HIPAA enforcement by increasing minimum and maximum potential CMPs for HIPAA violations. Pub. L. 111-5, section 13410, 123 Stat. 115, 271 (Feb. 17, 2009) (amending Social Security Act section 1176(a)(1), 42 U.S.C. 1320d-5(a)(1)). Section 13410(d) of the HITECH Act established four categories for HIPAA violations, with increasing penalty tiers based on the level of culpability associated with the violation: (1) the person did not know (and, by exercising reasonable diligence, would not have known) that the person violated the provision; (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. Thus, if a covered entity did not know that it violated HIPAA, and, through due care, would not

have known, the Secretary shall[1] impose "a penalty for each such violation of an amount that is at least the amount described in paragraph (3)(A) but not to exceed the amount described in paragraph (3)(D)[.]" 42 U.S.C. 1320d-5(a)(1)(A). Where the violation was due to reasonable cause, and not willful neglect, the Secretary shall impose "a penalty for each such violation of an amount that is at least the amount described in paragraph (3)(B) but not to exceed the amount described in paragraph (3)(D)[.]" *Id.* at section 1320d-5(a)(1)(B). If the violation were due to willful neglect, but was corrected in a timely manner, the Secretary shall impose "a penalty in an amount that is at least the amount described in paragraph (3)(C) but not to exceed the amount described in paragraph (3)(D)[.]" *Id.* at section 1320d-5(a)(1)(C)(i). And, finally, if the violation were due to willful neglect, but was not timely corrected, the Secretary shall impose "a penalty in an amount that is at least the amount described in paragraph (3)(D)." *Id.* at section 1320d-5(a)(1)(C)(ii).

The penalty amounts corresponding to each culpability level or violation type were set forth by the HITECH Act as follows:

> **Tiers of penalties described**.
>
> - the amount described in this subparagraph is $100 for each such violation, except that the total amount imposed on the person for all such violations of an identical requirement or prohibition during a calendar year may not exceed $25,000 (42 U.S.C. 1320d-5(a)(3)(A));
> - the amount described in this subparagraph is $1,000 for each such violation, except that the total amount imposed on the person for all such violations of an identical requirement or prohibition during a calendar year may not exceed $100,000 (42 U.S.C. 1320d-5(a)(3)(B));
> - the amount described in this subparagraph is $10,000 for each such violation, except that the total amount imposed on the

[1] 42 U.S.C. 1320d-5(a)(1) provides that "[e]xcept as provided in subsection (b) of this section, the Secretary shall impose on any person who violates a provision of this part . . . ."

person for all such violations of an identical requirement or prohibition during a calendar year may not exceed $250,000 (42 U.S.C. 1320d-5(a)(3)(C));

- the amount described in this subparagraph is $50,000 for each such violation, except that the total amount imposed on the person for all such violations of an identical requirement or prohibition during a calendar year may not exceed $1,500,000 (42 U.S.C. 1320d-5(a)(3)(D)).

On October 30, 2009, HHS issued an IFR to implement the enhanced penalty provisions of the HITECH Act. The Department's view at the time was that the HITECH Act's penalty provisions were "conflicting" because they allegedly referenced two levels of penalties for three of the four violation types. *See* HIPAA Administrative Simplification: Enforcement, 74 FR 56123, 56127 (Oct. 30, 2009). Although the HITECH Act provided four different annual penalty caps, the IFR concluded that "the most logical reading" of the law was to apply the highest annual cap of $1.5 million to all violation types, and that this was "consistent with Congress' intent to strengthen enforcement." *Id*.

On January 25, 2013, HHS adopted the text of the IFR as a final rule (Enforcement Rule) without change to the penalty tiers and annual limits. HHS noted in the preamble that, "[i]n adopting the HITECH Act's penalty scheme, the Department recognized that section 13410(d) contained apparently inconsistent language (*i.e.*, its reference to two penalty tiers 'for each violation,' each of which provided a penalty amount 'for all such violations' of an identical requirement or prohibition in a calendar year). To resolve this inconsistency, with the exception of violations due to willful neglect that are not timely corrected, the IFR adopted a range of penalty amounts between the minimum given in one tier and the maximum given in the second tier for each violation and adopted the amount of $1.5 million as the limit for all violations of an identical provision of the HIPAA rules in a calendar year." *See* Modifications to the HIPAA

Privacy, Security, Enforcement, and Breach Notification Rules Under the HITECH Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule, 78 FR 5566, 5582 (Jan. 25, 2013). The 2013 Enforcement Rule identified that some commenters expressed concern about the rule imposing a $1.5 million cap for every penalty tier. Such commenters argued that "the IFR's penalty scheme is inconsistent with the HITECH Act's establishment of different tiers based on culpability because the outside limits were the same for all culpability categories and this ignored the outside limits set forth by the HITECH Act within the lower penalty tiers, rendering those limits meaningless." 78 FR at 5583. In response, HHS stated that it continued to believe "that the penalty amounts are appropriate and reflect the most logical reading of the HITECH Act, which provides the Secretary with discretion to impose penalties for each category of culpability up to the maximum amount described in the highest penalty tier." *Id.*

As a result, the Enforcement Rule applies an annual upper limit of $1.5 million for each of the four culpability tiers, as shown below in Table 1.

Table 1: Penalty tiers under the Enforcement Rule

Culpability	**Minimum Penalty/Violation**	**Maximum Penalty/Violation**	**Annual Limit**
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

Upon further review of the statute by the HHS Office of the General Counsel, HHS has determined that the better reading of the HITECH Act is to apply annual limits as represented in Table 2 below: $25,000 for no knowledge, $100,000 for reasonable cause, $250,000 for corrected willful neglect, and $1,500,000 for uncorrected willful neglect. In light of this

determination, and as a matter of enforcement discretion, HHS is notifying the public that all HIPAA enforcement actions will be governed by the following interim penalty tiers:

Table 2: Penalty Tiers under Notification of Enforcement Discretion

Culpability	**Minimum Penalty/ Violation**	**Maximum Penalty/Violation**	**Annual Limit**
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 will use this penalty tier structure, as adjusted for inflation,[2] until further notice. *See, e.g.*, *Heckler v. Chaney*, 470 U.S. 821, 831 (1985) ("This Court has recognized on several occasions over many years that an agency's decision not to prosecute or enforce, whether through civil or criminal process, is a decision generally committed to an agency's absolute discretion.").

HHS expects to engage in future rulemaking to revise the penalty tiers in the current regulation to better reflect the text of the HITECH Act.

III. Collection of Information Requirements

This notification of enforcement discretion creates no legal obligations and no legal rights. Because this notification imposes no information collection requirements, it need not be reviewed by the Office of Management and Budget under the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 *et seq.*).

[2] HHS is required to annually adjust its CMPs for inflation pursuant to the cost-of-living formula set forth in the Federal Civil Penalties Inflation Adjustment Act Improvements Act of 2015, enacted as part of the Bipartisan Budget Act of 2015, Pub. L. No. 114-74, section 701, 129 Stat. 599 (Nov. 2, 2015).

Dated: April 23, 2019._____

Roger T. Severino,

Director, Office for Civil Rights,

Department of Health and Human Services.

[FR Doc. 2019-08530 Filed: 4/26/2019 4:15 pm; Publication Date: 4/30/2019]