

BENEFIT NEWS BRIEFS

A Look at the Civil Monetary Penalties for Violations of The HIPAA Privacy and Security Rules

Title XIII of the American Recovery and Reinvestment Act of 2009 (ARRA) is sometimes referred to as the "HITECH Act." [Section 13410 of the HITECH Act](#), summarized below, made the following changes to the penalties for violating the HIPAA administrative simplification provisions, which include the *HIPAA Privacy and Security Rules*. With the finalization of the regulations relative to civil penalties under Section 13410 of the *HITECH Act*, we thought we would take a look at the final regulation's tiered monetary penalties.

HITECH Act Section 13410: Improved Enforcement

This Section states a violation of a provision of ARRA that is due to *willful neglect* is a violation for which HHS is required to impose a penalty. HHS will formally investigate any complaint of such violation of this provision of ARRA if a preliminary investigation of the complaint indicates a possible violation due to "*willful neglect*."

There are also civil penalties for violations which the covered entity (health plan, healthcare clearinghouse or health care provider) or business associate:

- is not aware of, or would not be aware of through the exercise of reasonable diligence, or
- knew or could have known about, through the exercise of reasonable diligence, but did not know and which does not rise to the level of willful neglect.

Civil monetary penalties range from:

- \$100 per violation, not to exceed \$25,000 per year for the same type of violation;
- \$1,000 per violation if due to reasonable cause and not willful neglect, with a \$100,000 cap; and
- \$10,000 to \$50,000 in instances of willful neglect, with a \$250,000 to \$1.5 million cap.

There are also criminal penalties associated with *Privacy/Security Rule* violations that apply to knowingly and improperly disclosing or obtaining PHI under false pretenses. These criminal penalties are found in [42 U.S.C. Section 1320d-6](#) and are summarized below:

Criminal penalties range from:

- \$50,000 and one year in prison for intentionally obtaining or disclosing PHI;
- up to \$100,000 and up to five years in prison for obtaining PHI under "*false pretenses*"; and
- up to \$250,000 and up to 10 years in prison for obtaining or disclosing PHI with the intent to sell, transfer or use it for commercial advantage, personal gain or malicious harm.

Regulations implementing the tiered civil monetary penalties, and other *HITECH Act* changes, were published in the *Federal Register* on October 2009 and amended by further regulations published in January 2013.

The amount of monetary penalty which may be assessed under the regulations is set forth at [45 CFR Section 160.404](#). Sections 160.406 and 160.408 apply in determining the amount of the civil penalty assessed. Section 160.406 addresses violations of an identical requirement or prohibition and Section 160.408 addresses the consideration of certain mitigating or aggravating factors.

As a preliminary matter, the regulation at Section 160.401 sets forth some important definitions which are necessary to understanding the applicable civil penalties under Section 160.404.

Section 160.401 Definitions.

As used in this subpart, the following terms have the following meanings:

Reasonable cause means an act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the covered entity or business associate did not act with willful neglect.

Reasonable diligence means the business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances.

Willful neglect means conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated.

Section 160.404 Amount of a civil money penalty.

- (a) The amount of a civil money penalty will be determined in accordance with paragraph (b) of this Section and Sections 160.406, 160.408, and 160.412.
- (b) The amount of a civil money penalty that may be imposed is subject to the following limitations:

- (1) For violations occurring **prior to February 18, 2009**, the Secretary may not impose a civil money penalty-
 - (i) In the amount of *more than \$100* for each violation; or
 - (ii) *In excess of \$25,000* for identical violations during a calendar year (January 1 through the following December 31);
- (2) For violations occurring **on or after February 18, 2009**, the Secretary may not impose a civil money penalty-
 - (i) For a violation in which it is established that the covered entity or business associate *did not know* and, by exercising reasonable diligence, *would not have known* that the covered entity or business associate violated such provision,
 - (A) In the amount of *less than \$100 or more than \$50,000* for each violation; or
 - (B) *In excess of \$1,500,000* for identical violations during a calendar year (January 1 through the following December 31);
 - (ii) For a violation in which it is established that the violation was due to *reasonable cause* and *not to willful neglect*,
 - (A) In the amount of *less than \$1,000 or more than \$50,000* for each violation; or
 - (B) *In excess of \$1,500,000* for identical violations during a calendar year (January 1 through the following December 31);
 - (iii) For a violation in which it is established that the violation was *due to willful neglect* and *was corrected during the 30-day period* beginning on the first date the covered entity or business associate liable for the penalty knew, or, by exercising reasonable diligence, would have known that the violation occurred,
 - (A) In the amount of *less than \$10,000 or more than \$50,000* for each violation; or
 - (B) *In excess of \$1,500,000* for identical violations during a calendar year (January 1 through the following December 31);
 - (iv) For a violation in which it is established that the violation was *due to willful neglect* and *was not corrected during the 30-day period* beginning on the first date the covered entity or business associate liable for the penalty knew, or, by exercising reasonable diligence, would have known that the violation occurred,
 - (A) In the amount of *less than \$50,000* for each violation; or

- (B) *In excess of \$1,500,000* for identical violations during a calendar year (January 1 through the following December 31).
- (3) If a requirement or prohibition in one administrative simplification provision is repeated in a more general form in another administrative simplification provision in the same subpart, a civil money penalty may be imposed for a violation of only one of these administrative simplification provisions.

There are also regulations concerning the appeal rights of parties for which a civil monetary penalty is proposed. These regulations are found at [45 CFR 160.500-552](#).

More information on civil enforcement actions by the Office of Civil Rights (OCR), the *HIPAA Privacy and Security* enforcement arm of the Department of Health and Human Services (HHS), is available online at the OCR website located at: <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/index.html>.

* * *

LEGAL DISCLAIMER: Information contained in this publication is not legal advice, and should not be construed as legal advice. If you need legal advice upon which you can rely, you should seek a legal opinion from your attorney.