HIPAA Privacy and Security Rules: Enforcement

The Department of Health and Human Services (HHS), through its Office for Civil Rights (OCR), is responsible for enforcing the HIPAA Privacy and Security Rules. Although OCR has been enforcing HIPAA's rules since 2003, the Health Information Technology for Economic and Clinical Health (HITECH) Act, which was enacted as part of the American Recovery and Reinvestment Act of 2009, significantly enhanced OCR's enforcement authority.

Given this enhanced authority, there has been increased enforcement of the HIPAA Privacy and Security Rules recently with some costly outcomes for covered entities. OCR enforces the Privacy and Security Rules by investigating complaints that individuals file with it, conducting compliance reviews of covered entities and performing education and outreach to encourage compliance. OCR also works with the Department of Justice (DOJ) regarding possible criminal violations of HIPAA.

In addition, OCR has indicated that it may implement a permanent HIPAA audit program in the future.

LINKS AND RESOURCES

- HIPAA Enforcement Rule, which includes provisions relating to compliance and investigations, penalties and procedures.
- OCR's audit protocol, which includes the requirements that may be assessed during a HIPAA audit.
- Case examples of actual HIPAA enforcement action.

Enforcement Overview

OCR enforces compliance with the HIPAA Privacy and Security Rules for covered entities and their business associates (collectively, "regulated entities"). Covered entities include:

- Health plans;
- Health care clearinghouses; and
- Health care providers that transmit health information electronically in a transaction subject to HIPAA.

Most of OCR's investigations are trigged by individuals' complaints regarding HIPAA violations or a covered entity's breach notification reports. OCR has investigated many different types of entities, including national pharmacy chains, major medical centers, group health plans, hospital chains and small provider offices.

Enforcement Data

As of July 31, 2023, OCR has received over 336,404 HIPAA complaints and has initiated over 1,175 compliance reviews. OCR has resolved 98% of these cases (330,441). In many cases involving HIPAA violations, OCR worked with the entities involved to apply corrective measures instead of imposing penalties. However, to date, OCR has settled or imposed a civil money penalty in 135 of these cases, resulting in a total dollar amount of $135,538,772.

OCR's most investigated compliance issues (in order of frequency):

- Impermissible uses and disclosures of PHI;
- Lack of safeguards on PHI;
- Lack of patient access to PHI;

- Lack of administrative safeguards to protect electronic PHI (ePHI); and
- Uses or disclosures of more than the minimum necessary PHI.

HIPAA Audits

The HITECH Act requires HHS to perform periodic audits of covered entities and business associates to ensure their compliance with the HIPAA Rules.

- In 2011 and 2012, OCR implemented a pilot audit program to assess the controls and processes implemented by 115 covered entities to comply with HIPAA's requirements.
- In 2016 and 2017, OCR conducted the second phase of its HIPAA audit program. This second phase of HIPAA audits included both desk audits and onsite audits of covered entities and their business associates. On Dec. 17, 2020, OCR released its audit report for this phase of its audit program.
- OCR may implement a permanent HIPAA audit program, depending on the availability of agency resources.

According to OCR, these HIPAA audits are primarily a compliance improvement activity. However, if an audit reveals a serious compliance issue, OCR may initiate a compliance review to investigate.

This audit protocol can be used as a guide for internal self-audits of HIPAA compliance.

OCR updated its audit protocol in 2018to include the requirements that may be assessed during a HIPAA audit. The entire audit protocol is organized around modules, representing separate elements of privacy, security and breach notification. The combination of these multiple requirements may vary based on the type of covered entity or business associate selected for review.

Civil Penalties

HHS has the authority to assess **civil penalties** for violations of the HIPAA Privacy or Security Rules. The amount of the penalty depends on the type of violation involved. These penalties may not apply if the violation is corrected within 30 days of the date the person knew, or should have known, of the violation. HHS is also required to assess penalties for violations involving willful neglect and to formally investigate complaints of such violations.

These civil penalty amounts are subject to annual inflation-related increases. The penalty amounts that apply to civil penalties that are assessed on or after March 17, 2020 (and relate to violations occurring after Oct. 6, 2023 are as follows:

- ***Tier One:*** For violations where the covered entity or business associate does not know about the violation (and by exercising reasonable diligence, would not have known about the violation) the penalty amount is between $137 and $68,928 for each violation.
- ***Tier Two:*** If the violation is due to reasonable cause, the penalty amount is between $1,379 and $68,928 for each violation.
- ***Tier Three:*** For corrected violations that are caused by willful neglect, the penalty amount is between $13,785 and $68,928 for each violation.
- ***Tier Four:*** For violations caused by willful neglect that are not corrected, the penalty amount is $68,928 per violation, with an annual cap of $2,067,813 for all violations of an identical requirement.

Criminal Penalties

Criminal penalties may be assessed for violations of the HIPAA Privacy and Security Rules. These penalties are $50,000 and one year in prison for knowing violations, $100,000 and five years in prison for violations committed under false pretenses, and $250,000 and 10 years in prison for offenses committed for commercial or personal gain. Criminal actions may be brought against anyone who wrongly discloses PHI, not just covered entities or their employees.

Amount of Penalties - Important Factors

The Enforcement Rule provides some guidance on the actions that constitute a single violation, but gives HHS the authority to determine the number of violations based on the nature of the covered entity's obligation to act or not act under the provision that is violated. Where a violation is continuing, a separate violation occurs each day that the covered entity is in violation of the requirements.

Also, HHS must consider certain aggravating or mitigating factors when imposing civil penalties. These factors include the following:

- The nature and extent of the violation, including (but not limited to) the number of individuals affected and the time period during which the violation occurred;
- The nature and extent of the harm resulting from the violation, including whether the violation resulted in physical harm, financial harm, harm to an individual's reputation or hindered an individual's ability to obtain health care;

- The history of prior compliance with HIPAA's administrative simplification requirements, including whether the current violation is the same or similar to previous instances of noncompliance, whether and to what extent the covered entity has attempt to correct prior instances of noncompliance, how the covered entity has responded to technical compliance assistance from OCR and how the covered entity has responded to prior complaints;
- The financial condition and size of the covered entity; and
- Any other matters as justice may require.

Limits on Penalties

Civil money penalties may not be imposed if HHS determines that the violation was not due to willful neglect and it is corrected within a time frame specified by HHS (that is, within 30 days). Willful neglect is defined as a conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provisions. HHS has discretion to expand the 30-day time period depending on the nature and extent of the covered entity's compliance failure.

For violations due to reasonable cause and not to willful neglect that are not corrected in a timely manner, HHS may waive civil money penalties, in whole or in part, to the extent that payment of the penalty would be excessive relative to the violation. In addition, HHS must initiate civil money penalty actions within six years from the date the alleged violation occurred.

Third-Party Violations

The HITECH Act provides that HHS may impose penalties on "any person who violates a provision" of HIPAA's administrative simplification rules. The enforcement rules specifically indicate that HHS may impose civil money penalties against a covered entity for violations arising out of its workforce members' actions. Members of a covered entity's workforce include employees, volunteers, trainees or other individuals whose actions are under the covered entity's direct control.

In addition, civil penalties may be assessed against a covered entity for HIPAA violations committed by its business associate if the business associate is acting as the covered entity's agent. The key factor in determining whether an agency relationship exists is whether the covered entity has the authority to control the business associate's conduct in the course of performing a service on behalf of the covered entity. These penalties may apply even if a HIPAA-compliant business associate agreement is in place. Likewise, business associates are liable for the acts and omissions of their agents, including workforce members and subcontractors.

Investigative Process

The Enforcement Rule outlines a covered entity's obligations to cooperate with an investigation, the procedures related to hearings, including document discovery and HHS' ability to enforce and investigate a covered entity's compliance.

HHS has the authority to respond to complaints filed with its office as well as to initiate compliance reviews of covered entities. If OCR accepts a complaint for investigation, OCR will notify the person who filed the complaint and the covered entity identified in the complaint. OCR will ask the complainant and the covered entity to present information about the incident or problem described in the complaint. OCR may request specific information from each to get an understanding of the facts. Covered entities are required by law to cooperate with complaint investigations.

If a complaint describes an action that could be a violation of the criminal provision of HIPAA, OCR may refer the complaint to the DOJ for investigation.

OCR will review the information or evidence that it gathers in each case. In some cases, OCR may determine that the covered entity did not violate the requirements of the Privacy or Security Rule. If the evidence indicates that the covered entity was not in compliance, OCR will attempt to resolve the case with the covered entity by obtaining voluntary compliance, corrective action and/or a resolution agreement. OCR will notify the person who filed the complaint and the covered entity of the resolution result in writing.

Resolution Agreements

A resolution agreement is a settlement agreement signed by HHS and a covered entity or business associate in which the covered entity or business associate agrees to perform certain obligations and make reports to HHS, generally for a period of three years. During the period, HHS monitors the entity's compliance with its obligations. A resolution agreement may include the payment of a resolution amount. If HHS cannot reach a satisfactory resolution through the entity's demonstrated compliance or corrective action through other informal means, including a resolution agreement, civil money penalties may be imposed for noncompliance against a covered entity or business associate.