HIPAA violations & enforcement

U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) is responsible for enforcing the HIPAA Privacy and Security Rules.

OCR enforces the Privacy and Security Rules in several ways:

- Investigating complaints filed with it
- Conducting compliance reviews to determine if covered entities are in compliance
- Performing education and outreach to foster compliance with the rules' requirements

OCR reviews the information that it gathers. In some cases, it may determine that the covered entity did not violate the requirements of the Privacy and Security Rules. In the case of noncompliance, OCR will attempt to resolve the case with the covered entity by obtaining:

- Voluntary compliance
- Corrective action and/or
- Resolution agreement

Failure to comply with HIPAA can also result in civil and criminal penalties. If a complaint describes an action that could be a violation of the criminal provision of HIPAA, OCR may refer the complaint to the Department of Justice (DOJ) for investigation.

Civil violations

In cases of noncompliance where the covered entity does not satisfactorily resolve the matter, OCR may decide to impose civil money penalties (CMPs) on the covered entity.

CMPs for HIPAA violations are determined based on a tiered civil penalty structure. The secretary of HHS has discretion in determining the amount of the penalty based on the nature and extent of the violation and the nature and extent of the harm resulting from the violation. The secretary is prohibited from imposing civil penalties (except in cases of willful neglect) if the violation is corrected within 30 days (this time period may be extended at HHS’ discretion).

Penalties for civil violations

HIPAA violation: Unknowing Penalty range: $100 - $50,000 per violation, with an annual maximum of $25,000 for repeat violations

HIPAA violation: Reasonable Cause Penalty range: $1,000 - $50,000 per violation, with an annual maximum of $100,000 for repeat violations

HIPAA violation: Willful neglect but violation is corrected within the required time period Penalty range: $10,000 - $50,000 per violation, with an annual maximum of $250,000 for repeat violations

HIPAA violation: Willful neglect and is not corrected within required time period Penalty range: $50,000 per violation, with an annual maximum of $1.5 million

Criminal penalties

Criminal violations of HIPAA are handled by the DOJ. As with the HIPAA civil penalties, there are different levels of severity for criminal violations.

Covered entities and specified individuals, as explained below, who "knowingly" obtain or disclose individually identifiable health information, in violation of the Administrative Simplification Regulations, face a fine of up to $50,000, as well as imprisonment up to 1 year.

Offenses committed under false pretenses allow penalties to be increased to a $100,000 fine, with up to 5 years in prison.

Finally, offenses committed with the intent to sell, transfer or use individually identifiable health information for commercial advantage, personal gain or malicious harm permit fines of $250,000 and imprisonment up to 10 years.

Covered entities

Criminal penalties for HIPAA violations are directly applicable to covered entities (CE) including:

- Health plans
- Health care clearinghouses
- Health care providers who transmit claims in electronic form

- Medicare prescription drug card sponsors

Individuals such as directors, employees or officers of the CE (where the CE is not an individual) may also be directly criminally liable under HIPAA in accordance with "corporate criminal liability." Where an individual of a CE is not directly liable under HIPAA, they can still be charged with conspiracy or aiding and abetting.

Interpreting “knowingly”

The DOJ interpreted the "knowingly" element of the HIPAA statute for criminal liability as requiring only knowledge of the actions that constitute an offense. Specific knowledge of an action being in violation of the HIPAA statute is not required.

Exclusion from Medicare

HHS has the authority to exclude from participation in Medicare any CE that was not compliant with the transaction and code set standards by Oct. 16, 2003 (where an extension was obtained and the CE is not small) (68 FR 48805).

- HIPAA enforcement
- HIPAA security rule compliance
- Top tips for physicians (PDF)

This resource is provided for informational and reference purposes only and should not be construed as the legal advice of the American Medical Association. Specific legal questions regarding this information should be addressed by one's own counsel.