

# HIPAA Violations and Enforcement

Failure to comply with HIPAA can result in civil and criminal penalties (42 USC § 1320d-5).

## Civil Penalties

The “American Recovery and Reinvestment Act of 2009”(ARRA) that was signed into law on February 17, 2009, established a tiered civil penalty structure for HIPAA violations (see below). The Secretary of the Department of Health and Human Services (HHS) still 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 still 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).

HIPAA Violation	Minimum Penalty	Maximum Penalty
Individual did not know (and by exercising reasonable diligence would not have known) that he/she violated HIPAA	\$100 per violation, with an annual maximum of \$25,000 for repeat violations (Note: maximum that can be imposed by State Attorneys General regardless of the type of violation)	\$50,000 per violation, with an annual maximum of \$1.5 million
HIPAA violation due to reasonable cause and not due to willful neglect	\$1,000 per violation, with an annual maximum of \$100,000 for repeat violations	\$50,000 per violation, with an annual maximum of \$1.5 million
HIPAA violation due to willful neglect but violation is corrected within the required time period	\$10,000 per violation, with an annual maximum of \$250,000 for repeat violations	\$50,000 per violation, with an annual maximum of \$1.5 million
HIPAA violation is due to willful neglect and is not corrected	\$50,000 per violation, with an annual maximum of \$1.5 million	\$50,000 per violation, with an annual maximum of \$1.5 million

## Criminal Penalties

In June 2005, the U.S. Department of Justice (DOJ) clarified who can be held criminally liable under HIPAA. Covered entities and specified individuals, as explained below, whom "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 one year. Offenses committed under false pretenses allow penalties to be increased to a \$100,000 fine, with up to five 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 for up to ten years.

## Covered Entity and Specified Individuals

The DOJ concluded that the criminal penalties for a violation of HIPAA are directly applicable to covered entities—including health plans, health care clearinghouses, health care providers who transmit claims in electronic form, and Medicare prescription drug card sponsors. Individuals such as directors, employees, or officers of the covered entity, where the covered entity is not an individual, may also be directly criminally liable under HIPAA in accordance with principles of "corporate criminal liability." Where an individual of a covered entity is not directly liable under HIPAA, they can still be charged with conspiracy or aiding and abetting.

## 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.

### [Full DOJ memorandum](#)

(This link will take you off the AMA Web site. The AMA is not responsible for the content of other Web sites.)

## Exclusion

The Department of Health and Human Services (DHHS) has the authority to exclude from participation in Medicare any covered entity that was not compliant with the transaction and code set standards by October 16, 2003 (where an extension was obtained and the covered entity is not small) (68 FR 48805).

## Enforcing Agencies

The DHHS Office of Civil Rights (OCR) enforces the privacy standards, while the Centers for Medicare & Medicaid (CMS) enforces both the transaction and code set standards and the security standards (65 FR 18895). Enforcement of the civil monetary provisions has not yet been tasked to an agency.

Please refer to the AMA's [FAQs](#) on the privacy regulations for additional information on enforcement of the privacy standards.

## No Private Cause of Action

While HIPAA protects the health information of individuals, it does not create a private cause of action for those aggrieved (65 FR 82566). State law, however, may provide other theories of liability.