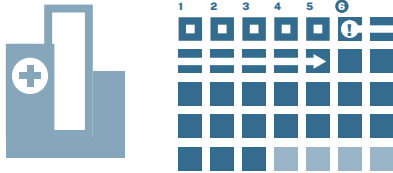


Penalties for HIPAA Violations Increase







The U.S. Department of Health and Human Services (HHS) has released its inflation-adjusted civil monetary penalties for violations of the HIPAA Privacy and Security Rules. The new amounts apply to penalties assessed **on or after Aug. 8, 2024**.

Because HIPAA's penalties are substantial, employers with group health plans should periodically review their compliance with the Privacy and Security Rules.

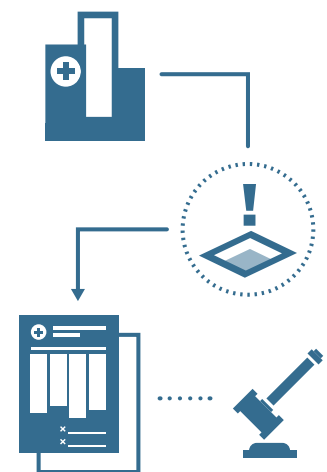
Increased Penalties

Potential penalties for HIPAA violations depend on the type of violation involved. Penalties are broken down into "tiers" that reflect increasing levels of culpability. Each tier carries a minimum and maximum penalty, all of which have increased as follows :

-  For violations where the covered entity or business associate did not know about the violation (and by exercising reasonable diligence, would not have known about the violation), the penalty amount is between **\$141** and **\$71,162** for each violation.
-  If the violation is due to reasonable cause, the penalty amount is between **\$1,424** and **\$71,162** for each violation.
-  For corrected violations that are caused by willful neglect, the penalty amount is between **\$14,232** and **\$71,162** for each violation.
-  For violations caused by willful neglect that are not corrected, the penalty amount is **\$71,162** for each violation, with an annual cap of **\$2,134,831**.

HIPAA Enforcement

HHS' Office for Civil Rights (OCR) is responsible for enforcing the HIPAA Privacy and Security Rules. When OCR determines that a HIPAA violation has occurred, it will often pursue a resolution agreement rather than imposing civil penalties. A resolution agreement typically requires a covered entity or business associate to take corrective action and pay a settlement amount, which is usually much less than the applicable penalty amount. However, if the covered entity or business associate does not take action to resolve the matter in a way that is satisfactory, OCR may decide to impose civil penalties.



Common HIPAA Violations

According to HHS, the compliance problems most frequently reported under HIPAA are:



Impermissible uses or disclosures of protected health information (PHI)



Lack of safeguards on PHI



Lack of patient access to their PHI



Lack of administrative safeguards for electronic PHI



Use or disclosure of more than the minimum necessary PHI