Provided by National Insurance Services

LEGAL UPDATE

HHS Increases Civil Penalties for HIPAA Violations

On Oct. 6, 2023, the U.S. Department of Health and Human Services (HHS) published a final rule increasing the civil monetary penalties for violations of the HIPAA Privacy and Security Rules. HHS is required to adjust these penalties for inflation each year to improve their effectiveness and maintain their deterrent effect. The new penalty amounts apply to penalties assessed on or after Oct. 6, 2023.

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

NIS
National Insurance Services

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

Inflation-adjusted 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 with an annual cap, all of which have increased as follows:

- **Tier One:** 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 $137 and $68,928 for each violation, with an annual cap of $2,067,813.
- **Tier Two:** If the violation is due to reasonable cause, the penalty amount is between $1,379 and $68,928 for each violation, with an annual cap of $2,067,813.
- **Tier Three:** For corrected violations that are caused by willful neglect, the penalty amount is between $13,785 and $68,928 for each violation, with an annual cap of $2,067,813.
- **Tier Four:** For violations caused by willful neglect that are not corrected, the penalty amount is $68,928 for each violation, with an annual cap of $2,067,813.

HIPAA Enforcement

HHS' Office for Civil Rights (OCR) is responsible for enforcing the HIPAA Privacy and Security Rules. OCR's investigations are often triggered by individuals' complaints to HHS regarding HIPAA violations and breach notification reports. 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. If penalties are imposed, the covered entity or business associate may request a hearing in which an HHS administrative law judge decides if the penalties are supported by the evidence in the case.