§ 150.315 Amount of penalty—General.

A civil money penalty for each violation of 42 U.S.C. 300gg et seq. may not exceed $100 for each day, for each responsible entity, for each individual affected by the violation. Penalties imposed under this part are in addition to any other penalties prescribed or allowed by law.

§ 150.317 Factors CMS uses to determine the amount of penalty.

In determining the amount of any penalty, CMS takes into account the following:

(a) The entity’s previous record of compliance. This may include any of the following:

(1) Any history of prior violations by the responsible entity, including whether, at any time before determination of the current violation or violations, CMS or any State found the responsible entity liable for civil or administrative sanctions in connection with a violation of HIPAA requirements.

(2) Documentation that the responsible entity has submitted its policy forms to CMS for compliance review.

(3) Evidence that the responsible entity has never had a complaint for noncompliance with HIPAA requirements filed with a State or CMS.

(4) Such other factors as justice may require.

(b) The gravity of the violation. This may include any of the following:

(1) The frequency of the violation, taking into consideration whether any violation is an isolated occurrence, represents a pattern, or is widespread.

(2) The level of financial and other impacts on affected individuals.

(3) Other factors as justice may require.

§ 150.319 Determining the amount of the penalty—mitigating circumstances.

For every violation subject to a civil money penalty, if there are substantial or several mitigating circumstances, the aggregate amount of the penalty is set at an amount sufficiently below the maximum permitted by §150.315 to reflect that fact. As guidelines for taking into account the factors listed in §150.317, CMS considers the following:

(a) Record of prior compliance. It should be considered a mitigating circumstance if the responsible entity has done any of the following:

(1) Before receipt of the notice issued under §150.307, implemented and followed a compliance plan as described in §150.311(f).

(2) Had no previous complaints against it for noncompliance.