

§ 150.307 Notice to responsible entities.

If an investigation under § 150.303 indicates a potential violation, CMS provides written notice to the responsible entity or entities identified under § 150.305. The notice does the following:

- (a) Describes the substance of any complaint or other information.
- (b) Provides 30 days from the date of the notice for the responsible entity or entities to respond with additional information, including documentation of compliance as described in § 150.311.
- (c) States that a civil money penalty may be assessed.

[64 FR 45795, Aug. 20, 1999, as amended at 70 FR 71023, Nov. 25, 2005]

§ 150.309 Request for extension.

In circumstances in which an entity cannot prepare a response to CMS within the 30 days provided in the notice, the entity may make a written request for an extension from CMS detailing the reason for the extension request and showing good cause. If CMS grants the extension, the responsible entity must respond to the notice within the time frame specified in CMS's letter granting the extension of time. Failure to respond within 30 days, or within the extended time frame, may result in CMS's imposition of a civil money penalty based upon the complaint or other information alleging or indicating a violation of HIPAA requirements.

§ 150.311 Responses to allegations of noncompliance.

In determining whether to impose a civil money penalty, CMS reviews and considers documentation provided in any complaint or other information, as well as any additional information provided by the responsible entity to demonstrate that it has complied with HIPAA requirements. The following are examples of documentation that a potential responsible entity may submit for CMS's consideration in determining whether a civil money penalty should be assessed and the amount of any civil money penalty:

- (a) Any individual policy, group policy, certificate of insurance, application, rider, amendment, endorsement, certificate of creditable coverage, ad-

vertising material, or any other documents if those documents form the basis of a complaint or allegation of noncompliance, or the basis for the responsible entity to refute the complaint or allegation.

- (b) Any other evidence that refutes an alleged noncompliance.

- (c) Evidence that the entity did not know, and exercising due diligence could not have known, of the violation.

- (d) Documentation that the policies, certificates of insurance, or non-Federal governmental plan documents have been amended to comply with HIPAA requirements either by revision of the contracts or by the development of riders, amendments, or endorsements.

- (e) Documentation of the entity's issuance of conforming policies, certificates of insurance, plan documents, or amendments to policyholders or certificate holders before the issuance of the notice to the responsible entity or entities described in § 150.307.

- (f) Evidence documenting the development and implementation of internal policies and procedures by an issuer, or non-Federal governmental health plan or employer, to ensure compliance with HIPAA requirements. Those policies and procedures may include or consist of a voluntary compliance program. Any such program should do the following:

- (1) Effectively articulate and demonstrate the fundamental mission of compliance and the issuer's, or non-Federal governmental health plan's or employer's, commitment to the compliance process.

- (2) Include the name of the individual in the organization responsible for compliance.

- (3) Include an effective monitoring system to identify practices that do not comply with HIPAA requirements and to provide reasonable assurance that fraud, abuse, and systemic errors are detected in a timely manner.

- (4) Address procedures to improve internal policies when noncompliant practices are identified.

- (g) Evidence documenting the entity's record of previous compliance with HIPAA requirements.

[64 FR 45795, Aug. 20, 1999, as amended at 70 FR 71023, Nov. 25, 2005]