

penalty, irrespective of whether a civil money penalty is imposed under paragraph (a) of this section. The employer is the responsible entity irrespective of whether the plan is administered by a health insurance issuer, the employer, or a third-party administrator.

(2) *Exception.* In the case of a non-Federal governmental plan that is not provided through health insurance coverage, this paragraph (c) does not apply to the extent the non-Federal governmental employer has elected under § 146.180 to exempt the plan from applicable HIPAA requirements.

(d) *Actions or inactions of agent.* A principal is liable for penalties assessed for the actions or inactions of its agent.

§ 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. (See Appendix A to this subpart for examples of violations.)

(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.

§ 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, advertising 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 of intent to assess a penalty 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-

§ 150.313

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.

§ 150.313 Market conduct examinations.

(a) *Definition.* A market conduct examination means the examination of health insurance operations of an issuer, or the operation of a non-Federal governmental plan, involving the review of one or more (or a combination) of a responsible entity's business or operational affairs, or both, to verify compliance with HIPAA requirements.

(b) *General.* If, based on the information described in §150.303, CMS finds evidence that a specific entity may be in violation of a HIPAA requirement, CMS may initiate a market conduct examination to determine whether the entity is out of compliance. CMS may conduct the examinations either at the site of the issuer or other responsible entity or a site CMS selects. When CMS selects a site, it may direct the issuer or other responsible entity to forward any documentation CMS considers relevant for purposes of the examination to that site.

(c) *Appointment of examiners.* When CMS identifies an issue that warrants investigation, CMS will appoint one or more examiners to perform the examination and instruct them as to the scope of the examination.

(d) *Appointment of professionals and specialists.* When conducting an examination under this part, CMS may retain attorneys, independent actuaries, independent market conduct examiners, or other professionals and specialists as examiners.

45 CFR Subtitle A (10-1-03 Edition)

(e) *Report of market conduct examination.* (1) *CMS review.* When CMS receives a report, it will review the report, together with the examination work papers and any other relevant information, and prepare a final report. The final examination report will be provided to the issuer or other responsible entity.

(2) *Response from issuer or other responsible entity.* With respect to each examination issue identified in the report, the issuer or other responsible entity may:

(i) Concur with CMS's position(s) as outlined in the report, explaining the plan of correction to be implemented.

(ii) Dispute CMS's position(s), clearly outlining the basis for its dispute and submitting illustrative examples where appropriate.

(3) *CMS's reply to a response from an issuer or other responsible entity.* Upon receipt of a response from the issuer or other responsible entity, CMS will provide a letter containing its reply to each examination issue. CMS's reply will consist of one of the following:

(i) Concurrence with the issuer's or non-Federal governmental plan's position.

(ii) Approval of the issuer's or non-Federal governmental plan's proposed plan of correction.

(iii) Conditional approval of the issuer's or non-Federal governmental plan's proposed plan of correction, which will include any modifications CMS requires.

(iv) Notice to the issuer or non-Federal governmental plan that there exists a potential violation of HIPAA requirements.

§ 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: