

- Recommendations to minimize the information collection burden on the affected public, including automated collection techniques.

As discussed below, we are soliciting comment on the recordkeeping requirements, as referenced in § 164.306, § 164.308, § 164.310, § 164.314, and § 164.316 of this document.

Section 164.306 Security Standards: General Rules

Under paragraph (d), a covered entity must, if implementing the implementation specification is not reasonable and appropriate, document why it would not be reasonable and appropriate to implement the implementation specification.

We estimate that 75,000 entities will be affected by this requirement and that they will have to create documentation 3 times for this requirement. We estimate each instance of documentation will take .25 hours, for a one-time total burden of 56,250 hours.

Section 164.308 Administrative Safeguards

Under this section, a covered entity must document known security incidents and their outcomes.

We estimate that there will be 50 known incidents annually and that it will take 8 hours to document this requirement, for an annual burden of 400 hours.

This section further requires that each entity have a contingency plan, with specified components.

We estimate that there will be 60,000 entities affected by this requirement and that it will take each entity 8 hours to comply, for a total one-time burden of 480,000 hours.

This section also requires that the written contract or other arrangement with a business associate document the satisfactory assurances that the business associate will appropriately safeguard the information through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a).

We believe that the burden associated with this requirement is not subject to the PRA. It is good business practice for entities to document their arrangements via written contracts and as such is usual and customary among the entities subject to them. A burden associated with a requirement conducted in the normal course of business is exempt from the PRA as defined in 5 CFR 1320.3(b)(2).

Section 164.310 Physical Safeguards

This section requires that a covered entity implement policies and procedures to document repairs and modifications to the physical components of a facility that are related to security (for example, hardware, walls, doors, and locks).

We believe that 15,500 entities will have to repair or modify physical components, most of which will need to be done in the first year of implementation. In the following years, we estimate that 500 entities will need to make repairs or modifications. We estimate that it will take 10 minutes to document each repair or modification for a burden of 2,583 hours the first year and 83 hours annually subsequently.

This section requires that a covered entity create a retrievable, exact copy of electronic protected health information, where needed, before movement of equipment.

We believe that the burden associated with this requirement is not subject to the PRA. It is good business practice for entities to backup their data files, and as such is usual and customary among the entities subject to them. A burden associated with a requirement conducted in the normal course of business is exempt from the PRA as defined in 5 CFR 1320.3(b)(2).

Section 164.314 Organizational Requirements

This section requires that a covered entity report to the Secretary problems with a business associate's pattern of an activity or practice of the business associate that constitute a material breach or violation of the business associate's obligation under the contract or other arrangement if it is not feasible to terminate the contract or arrangement.

We believe that 10 entities will need to comply with this reporting requirement and that it will take them 60 minutes to comply with this requirement for an annual burden of 10 hours.

This section also requires that a covered entity may, if a business associate is required by law to perform a function or activity on behalf of a covered entity or to provide a service described in the definition of business associate as specified in § 160.103 of this subchapter to a covered entity, permit the business associate to create, receive, maintain, or transmit electronic protected health information on its behalf to the extent necessary to comply with the legal mandate without meeting the requirements of paragraph (a)(2)(i) of this section, provided that the covered

entity attempts in good faith to obtain satisfactory assurances as required by paragraph (a)(2)(ii)(A) of this section, and documents the attempt and the reasons that these assurances cannot be obtained.

We believe that this situation will affect 20 entities and that it will take 60 minutes to document attempts to obtain assurances and the reasons they cannot be obtained for an annual burden of 20 hours.

This section further requires that business associate contracts or other arrangements and group health plans must require the business entity and plan sponsor, respectively, to report to the covered entity any security incident of which it becomes aware.

We believe that the burden associated with this requirement is not subject to the PRA. It is good business practice for entities to document their agreements via written contracts, and as such is usual and customary among the entities subject to them. A burden associated with a requirement conducted in the normal course of business is exempt from the PRA as defined in 5 CFR 1320.3(b)(2).

Section 164.316 Policies and Procedures and Documentation Requirements

Paragraph (b)(1), *Standard: Documentation*, of this section requires a covered entity to—

(i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and

(ii) If an action, activity, assessment, or designation is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, assessment, or designation.

We estimate that it will take the 4,000,000 entities covered by this final rule 16 hours to document their policies and procedures, for a total one-time burden of 64,000,000 hours.

The total annual burden of the information collection requirements contained in this final rule is 64,539,264 hours. These information collection requirements will be submitted to OMB for review under the PRA and will not become effective until approved by OMB.

If you comment on these information collection and recordkeeping requirements, please mail copies directly to the following:

Centers for Medicare and Medicaid Services, Office of Strategic Operations and Regulatory Affairs, Regulations Development and Issuances Group, Attn: Reports