

Clearance Officer, 7500 Security Boulevard, Baltimore, MD 21244–1850, Attn: Julie Brown, CMS–0049–F; and
Office of Information and Regulatory Affairs, Office of Management and Budget, Room 10235, New Executive Office Building, Washington, DC 20503, Attn: Brenda Aguilar, CMS Desk Officer.

IV. Regulatory Impact Analysis

A. Overall Impact

We have examined the impacts of this rule as required by Executive Order 12866 (September 1993, Regulatory Planning and Review), the Regulatory Flexibility Act (RFA) (September 16, 1980, Pub. L. 96–354), section 1102(b) of the Social Security Act, the Unfunded Mandates Reform Act of 1995 (Pub. L. 104–4), and Executive Order 13132.

Executive Order 12866 (as amended by Executive Order 13258, which merely reassigns responsibility of duties) directs agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). A regulatory impact analysis (RIA) must be prepared for major rules with economically significant effects (\$100 million or more in any 1 year). Although we cannot determine the specific economic impact of the standards in this final rule (and individually each standard may not have a significant impact), the overall impact analysis makes clear that, collectively, all the standards will have a significant impact of over \$100 million on the economy. Because this rule affects over 2 million entities, a requirement as low as \$50 per entity would render this rule economically significant. This rule requires each of these entities to engage in, for example, at least some risk assessment activity; thus, this rule is almost certainly economically significant even though we do not have an estimate of the marginal impact of the additional security standards. However, the standards adopted in this rule are considerably more flexible than those anticipated in the overall impact analysis. Therefore, their implementation costs should be lower than those assumed in the impact analysis.

The RFA requires agencies to analyze options for regulatory relief of small businesses. For purposes of the RFA, small entities include small businesses,

nonprofit organizations, and government agencies. Most hospitals and most other providers and suppliers are small entities, either by nonprofit status or by having revenues of \$6 million to \$29 million in any 1 year. While each standard may not have a significant impact on a substantial number of small entities, the combined effects of all the standards are likely to have a significant effect on a substantial number of small entities. Although we have certified this rule as having a significant impact, we have previously discussed the impact of small entities in the RFA published as part of the August 17, 2000 final regulation for the Standards for Electronic Transactions (65 FR 50312), on pages 50359 through 50360. That analysis included the impact of the set of HIPAA standards regulations (transactions and code sets, identifiers, and security). Although we discussed the impact on small entities in the previous analysis, we would like to discuss how this final rule has been structured to minimize the impact on small entities, compared to the proposed rule.

The proposed rule mandated 69 implementation features for all entities. A large number of commenters indicated that mandating such a large number would be burdensome for all entities. As a result, we have restructured this final rule to permit greater flexibility. While all standards must be met, we are now only requiring 13 implementation specifications. The remainder of the implementation specifications is “addressable.” For addressable specifications, an entity decides whether each specification is a reasonable and appropriate security measure to apply within its particular security framework. This decision is based on a variety of factors, for example, the entity’s risk analysis, what measures are already in place, the particular interest to small entities, and the cost of implementation.

Based on the decision, an entity can—(1) implement the specification if reasonable and appropriate; (2) implement an alternative security measure to accomplish the purposes of the standard; or (3) not implement anything if the specification is not reasonable and appropriate and the standard can still be met.

This approach will provide flexibility for all entities, and especially small entities that would be most concerned about the cost and complexity of the security standards. Small entities can look at the addressable implementation specifications and tailor their compliance based on their risks and capabilities of addressing those risks.

The required risk analysis is also a tool to allow flexibility for entities in meeting the requirements of this final rule. The risk analysis requirement is designed to allow entities to look at their own operations and determine the security risks involved. The degree of response is determined by the risks identified. We assume that smaller entities, who deal with smaller amounts of information would have smaller physical facilities, smaller work forces, and therefore, would assume less risk. The smaller amount of risk involved means that the response to that risk can be developed on a smaller scale than that for larger organizations.

Individuals and States are not included in the definition of a small entity. However, the security standards will affect small entities, such as providers and health plans, and vendors in much the same way as they affect any larger entities. Small providers who conduct electronic transactions and small health plans must meet the provisions of this regulation and implement the security standards. A more detailed analysis of the impact on small entities is part of the impact analysis published on August 17, 2000 (65 FR 50312), which provided the impact for all of the HIPAA standards, except privacy. As we discussed above, the scalability factor of the standards means that the requirements placed upon small providers and plans would be consistent with the complexity of their operations. Therefore, small providers and plans with appropriate security processes in place would need to do relatively little in order to comply with the standards. Moreover, small plans will have an additional year to come into compliance.

In addition, section 1102(b) of the Act requires us to prepare a regulatory impact analysis if a rule may have a significant impact on the operations of a substantial number of small rural hospitals. This analysis must conform to the provisions of section 604 of the RFA. For purposes of section 1102(b) of the Act, we define a small rural hospital as a hospital that is located outside of a Metropolitan Statistical Area and has fewer than 100 beds. While this rule may have a significant impact on small rural hospitals, the impact should be minimized by the scalability factors of the standards, as discussed above in the impact on all small entities. In addition, we have previously discussed the impact of small entities in the RIA published as part of the August 17, 2000 final regulation for the Standards for Electronic Transactions.

Section 202 of the Unfunded Mandates Reform Act (UMRA) of 1995