

HHS cost estimates should be publicized for comparison purposes.

Still another commenter stated that HHS must provide accurate public sector implementation cost figures and provide funds to offset the cost burden.

One commenter asked for cost benefit evaluations to understand the relationship between competing technologies, levels of security and potential threats to be guarded against. These would demonstrate the costs and the benefits to be gained for both large and small organizations and would provide an understanding of how the levels of security vary by organization size and what the inducements and support available to facilitate adoption are. One commenter suggested that we establish a workgroup to more fully assess the costs and provide Federal funds to offset implementation costs.

One commenter noted a seeming disconnect between two statements in the preamble. Section A, Security standards, states, "no individual small entity is expected to experience direct costs that exceed benefits as a result of this rule." In contrast, section E, Factors in establishing the security standards reads, "We cannot estimate the per-entirety cost of implementation because there is no information available regarding the extent to which providers', plans', and clearinghouses' current security practices are deficient."

*Response:* We are unable to estimate, of the nation's 2 million-plus health plans and 1 million-plus providers that conduct electronic transactions, the number of entities that would require new or modified security safeguards and procedures beyond what they currently have in place. Nor are we able to estimate the number of entities that neither conduct electronic transactions nor maintain individually identifiable electronic health information but may become covered entities at some future time. As we are unable to estimate the number of entities and what measures are or are not already in place, or what specific implementation will be chosen to meet the requirements of the regulation, we are also unable to estimate the cost to those entities.

However, the use of electronic technology to maintain or transmit health information results in many new and potentially large risks. These risks represent expected costs, both monetary and social. Leaving risk assessment up to individual entities will minimize the impact and ensure that security effort is proportional to security risk.

As discussed earlier, the security requirements are both scalable and technically flexible. We have made significant changes to this final rule,

reducing the number of required implementation features and providing for greater flexibility in satisfaction of the requirements. In other words, we have focused more on what needs to be done and less on how it should be accomplished.

We have removed the statement regarding the extent of costs versus benefits for small entities.

b. *Comment:* One commenter stated that on page 43262 of the proposed rule, it indicate that complexity of conversion to the security standards would be affected by the choice to use a clearinghouse. The commenter stated that this choice would have little effect on implementation of security standards. Another commenter stated that the complexity (and cost) of the conversion to meet the security standards is affected by far more than just the "volume of claims health plans process electronically and the desire to transmit the claims or to use the services of a VAN or clearinghouse" as is stated on page 43262. Because the security standards apply to internal systems as well as to transactions between entities, a number of additional factors must be considered, for example, modification of existing security mechanisms, legacy systems, architecture, and culture.

*Response:* We agree. We have modified the Regulatory Impact Analysis section to take into account that there are other factors involved, such as the architecture and technology limitations of existing systems.

c. *Comment:* One commenter stated that States will need 90 percent funding of development and implementation, without the burden of an advanced planning documents requirement, from us for this costly process to succeed. Any new operational obligation should be 100 percent funded. Also human resource obligations will be significant. Some States believe they will have difficulty obtaining the budget funds for the State share of the costs. State Medicaid agencies, as purchasers, may also face paying the implementation costs of health care providers, clearinghouses, and health plans in the form of higher rates.

*Response:* The statute does not authorize any new or special funding for implementation of the regulations. Medicaid system changes, simply because they are "HIPAA related" do not automatically qualify for 90 percent Federal funding participation. As with any systems request, the usual rules will be applied to determine funding eligibility for State HIPAA initiatives. Nevertheless, HHS recognizes that there are significant issues regarding the

funding and implementation of HIPAA by Medicaid State agencies, and intends to address them through normal channels of communication with States.

d. *Comment:* One commenter stated that the proposed rule does not establish how the security standards will contribute to reduced cost for providers. One commenter expected the unintended result of this regulation will be impediment of EDI growth and perhaps even a decline in EDI use by providers. Another stated that the proposed rule actively discourages physician EDI participation by suggesting a fallback to paper processing for those unable to meet the cost of highly complex security compliance.

*Response:* Ensuring the integrity of an electronic message, its delivery to the correct person, and its confidentiality must be an integral part of conducting electronic commerce. We believe that the consistent application of the measures provided in this rule will actually encourage use of EDI because it will provide increased confidence in the reliability and confidentiality of health information to all parties involved.

Also, the implementation of these security requirements will reduce the potential overall cost of risk to a greater extent than additional security controls will increase costs. Put another way, the potential cost of not reasonably addressing security risks could substantially exceed the cost of compliance.

e. *Comment:* One commenter stated that the implementation impact of the technical safeguards is clearly understated for physicians who use digitally-based equipment that has been in place for some time. The commenter believes that the rule will likely have greatest impact on the installed base of digital systems, including imaging modalities and other medical devices that store or transmit patient information because software for legacy systems will likely require retrofitting or replacement to come into compliance. The commenter believes that this is a negative impact and would outweigh any benefits derived from the potential risk of security breaches. The commenter recommended compliance for digital imaging devices be extended by an additional 3 years to allow time to upgrade systems and defray the associated costs.

*Response:* Compliance dates for the initial implementation of the initial standards are statutorily prescribed; therefore, we are unable to allow additional time outside of the statutory timeframes for compliance.

f. *Comment:* A commenter stated that, as a new regulatory mandate, HIPAA