

limitations of existing systems could also affect the complexity of the conversion (for example, certain practice management software that does not contain password protection will require a greater conversion effort than software that has a password protection option already built into it).

### 3. Cost of Conversion

Virtually all providers, health plans, and clearinghouses that transmit or store data electronically have already implemented some security measures and will need to assess existing security, identify areas of risk, and implement additional measures in order to come into compliance with the standards adopted in this rule. We cannot estimate the per-entity cost of implementation because there is no information available regarding the extent to which providers', plans', and clearinghouses' current security practices are deficient. Moreover, some security solutions are almost cost-free to implement (for example, reminding employees not to post passwords on their monitors), while others are not.

Affected entities will have many choices regarding how they will implement security. Some may choose to assess security using in-house staff, while others will use consultants. Practice management software vendors may also provide security consultation services to their customers. Entities may also choose to implement security measures that require hardware and/or software purchases at the time they do routine equipment upgrades.

The security standards we adopt in this rule were developed with considerable input from the health care industry, including providers, health plans, clearinghouses, vendors, and standards organizations. Industry members strongly advocated the flexible approach we adopt in this rule, which permits each affected entity to develop cost-effective security measures appropriate to their particular needs. We believe that this approach will yield the lowest implementation cost to industry while ensuring that electronic protected health information is safeguarded.

All of the nation's health plans (over 2 million) and providers (over 600,000) will need to conduct some level of gap analysis to assess current procedures against the standards. However, we cannot estimate the number of covered entities that would have to implement additional security systems and procedures to meet the adopted standards. Also, we are not able to estimate the number of providers that do not conduct electronic transactions

today but may choose to do so at some future time (these would be entities that send and receive paper transactions and maintain paper records and thus would not be affected). We believe that the security standards represent the minimum necessary for adequate protection of health information in an electronic format and as such should be implemented by all covered entities. As discussed earlier in this preamble, the security requirements are both scalable and technically flexible; and while the law requires each health plan that is not a small plan to comply with the security and electronic signature requirements no later than 24 months after the effective date of the final rule, small plans will be allowed an additional 12 months to comply.

Since we are unable to estimate the number of entities that may need to make changes to meet the security standards, we are also unable to estimate the cost for those entities. However, we believe that the cost of establishing security systems and procedures is a portion of the costs associated with converting to the administrative simplification standards that are required under HIPAA, which are estimated in the previously referenced impact analysis.

This discussion on conversion costs relates only to health plans, health care providers, and health care clearinghouses that are required to implement the security standards. The cost of implementing security systems and procedures for entities that do not transmit, receive, or maintain health information electronically is not a cost imposed by the rule, and thus, is not included in our estimates.

### G. Alternatives Considered

In developing this final rule, the Department considered some alternatives. One alternative was to not issue a final rule. However, this would not meet the Department's obligations under the HIPAA statute. It would also leave the health industry without a set of standards for protecting the security of health information. The vast majority of commenters supported our efforts in developing a set of standards. Thus, we concluded that not publishing a final rule was not in the best interests of the industry and not in the best interests of persons whose medical information will be protected by these measures.

A second alternative was to publish the final rule basically unchanged from the proposed rule. Although most commenters supported the approach of the proposed rule, there were significant objections to the number of required specifications, concerns about the scope

of certain requirements, duplication and ambiguity of some requirements, and the overall complexity of the approach. Based on those comments, it was clear that revisions had to be made. In addition, the proposed rule was developed before the Privacy Rule requirements were developed. Thus, it did not allow for any alignment of requirements between the Privacy and Security standards.

As a result, the Department determined that an approach that modified the proposed rule and aligned the requirements with the Privacy standards was the preferred alternative.

### V. Federalism

Executive Order 13132 of August 4, 1999, Federalism, published in the **Federal Register** on August 10, 1999 (64 FR 43255), requires us to ensure meaningful and timely input by State and local officials in the development of rules that have Federalism implications. Although the proposed rule for security standards was published before the enactment of this Executive Order, the Department consulted with State and local officials as part of an outreach program in the process of developing the proposed regulation. The Department received comments on the proposed rule from State agencies and from entities that conduct transactions with State agencies. Many of these comments were concerned with the burden that the proposed security standards would place on their organizations. In response to those comments, we have modified the security standards to make them more flexible and less burdensome.

In complying with the requirements of part C of Title XI, the Secretary established an interdepartmental team who consulted with appropriate State and Federal agencies and private organizations. These external groups included the NCVHS Workgroup on Standards and Security, the Workgroup for Electronic Data Interchange, the National Uniform Claim Committee, and the National Uniform Billing Committee. Most of these groups have State officials as members. We also received comments on the proposed regulation from these organizations.

In accordance with the provisions of Executive Order 12866, this rule has been reviewed by the Office of Management and Budget.

### List of Subjects

#### 45 CFR Part 160

Electronic transactions, Employer benefit plan, Health, Health care, Health facilities, Health insurance, Health