

principle establishes a performance objective for the standard.

- Be technologically independent of the computer platforms and transmission protocols used in health transactions, except when they are explicitly part of the standard. This principle establishes a performance objective for the standard and supports the regulatory goal of flexibility.

- Be precise and unambiguous but as simple as possible. This principle supports the regulatory goals of predictability and simplicity.

- Keep data collection and paperwork burdens on users as low as is feasible. This principle supports the regulatory goals of cost-effectiveness and avoidance of duplication and burden.

- Incorporate flexibility to adapt more easily to changes in the health care infrastructure (for example, new services, organizations, and provider types) and information technology. This principle supports the regulatory goals of flexibility and encouragement of innovation.

We assessed a wide variety of security standards and guidelines against the principles listed above, with the overall goal of achieving the maximum benefit for the least cost. As we stated in the proposed rule, we found that no single standard for security exists that encompasses all the requirements that were listed in the law. However, we believe that the standards we are adopting in this final rule collectively accomplish these goals.

#### *E. Affected Entities*

##### 1. Health Care Providers

Covered health care providers may incur implementation costs for establishing or updating their security systems. The majority of costs to implement the security standard (purchase and installation of appropriate computer hardware and software, and physical safeguards) would generally be incurred in the initial implementation period for the specific requirements of the security standard. Health care providers that do not conduct electronic transactions for which standards have been adopted are not affected by these regulations.

##### 2. Health Plans

All health plans, as the term is defined in regulation at 45 CFR 160.103, must comply with these security standards. In addition, health plans that engage in electronic health care transactions may have to modify their systems to meet the security standards. Health plans that maintain electronic health information may also have to

modify their systems to meet the security standards. This conversion would have a one-time cost impact on Federal, State, and private plans alike.

We recognize that this conversion process has the potential to cause business disruption of some health plans. However, health plans would be able to schedule their implementation of the security standards and other standards in a way that best fits their needs, as long as they meet the deadlines specified in the HIPAA law and regulations. Moreover, small plans (many of which are employer-sponsored) will have an additional year in which to achieve compliance. Small health plans are defined at 45 CFR 160.103 as health plans with annual receipts of \$5 million or less.

##### 3. Clearinghouses

All health care clearinghouses must meet the requirements of this regulation. Health care clearinghouses would face effects similar to those experienced by health care providers and health plans. However, because clearinghouses represent one way in which providers and plans can achieve compliance, the clearinghouses' costs of complying with these standards would probably be passed along to those entities, to be shared over the entire customer base.

##### 4. System Vendors

Systems vendors that provide computer software applications to health care providers and other billers of health care services would likely be affected. These vendors would have to develop software solutions that would allow health plans, providers, and other users of electronic transactions to protect these transactions and the information in their databases from unauthorized access to their systems. Their costs would also probably be passed along to their customer bases.

#### *F. Factors in Establishing the Security Standard*

##### 1. General Effect

In assessing the impact of these standards, it is first necessary to focus on the general nature of the standards, their scalability, and the fact that they are not dependent upon specific technologies. These factors will make it possible for covered entities to implement them with the least possible impact on resources. Because there is no national security standard in widespread use throughout the industry, adopting any of the candidate standards would require most health care providers, health plans, and health care clearinghouses to at least conduct

an assessment of how their current security measures conform to the new standards. However, we assume that most, if not all, covered entities already have at least some rudimentary security measures in place. Covered entities that identify gaps in their current measures would need to establish or revise their security precautions.

It is also important to note that the standards specify what goals are to be achieved, but give the covered entity some flexibility to determine how to meet those goals. This is different from the transaction standards, where all covered entities must use the exact same implementation guide. With respect to security, covered entities will be able to blend security processes now in place with new processes. This should significantly reduce compliance costs.

Based on our analysis and comments received, the security standards adopted in this rule do not impose a greater burden on the industry than the options we did not select, and they present significant advantages in terms of universality and flexibility.

We understand that some large health plans, health care providers, and health care clearinghouses that currently exchange health information among trading partners may already have security systems and procedures in place to protect the information from unauthorized access. These entities may not incur significant costs to meet the security standards. Large entities that have sophisticated security systems in place may only need minor revisions or updates to their systems to meet the security standards, or indeed, may not need to make any changes in their systems.

While small providers are not likely to have implemented sophisticated security measures, they are also not as likely to need them as larger covered entities. The scalability principle allows providers to adopt measures that are appropriate to their own circumstances.

##### 2. Complexity of Conversion

The complexity of the conversion to the security standards could be significantly affected by the volume of transactions that covered entities transmit and process electronically and the desire to transmit directly or to use the services of a Value Added Network (VAN) or a clearinghouse. If a VAN or clearinghouse is used, some of the conversion activities would be carried out by that organization, rather than by the covered entity. This would simplify conversion for the covered entity, but makes the covered entity dependent on the success of its business associate. The architecture, and specific technology