

technologies to protect information have been developed over the past several years. As a result, HHS has consulted with the Gartner Group, a leading technology assessment organization, regarding what impact these changes in the industry might have on the expected impact of this regulation. The Gartner analysis indicated that the cost of meeting the requirements of a reasonable interpretation of the security rule in 2002 is probably less than 10 percent higher in 2002 than it was in 1998. This increase is mainly driven by more active threats and increased personnel costs offsetting decreases in technology costs over the past 4 years. However, spending by companies who have anticipated the security rule or who have independently made business decisions to implement security policies and procedures as good business practice(s) has already occurred, and probably will cancel out the increased costs of implementation. Therefore, Gartner expects the cost of complying with the HIPAA security standards to be about the same now as it was in 1998.

## 2. Synchronizing Standards

The timelines for the implementation of the initial HIPAA standards (transactions, identifiers, and security) are no longer closely synchronized. However, we do not believe that this lack of synchronization will have a significant impact on the cost of implementing security. The analysis provided by the Gartner group indicated that implementing security standards is being viewed by entities as a separate task from implementing the transaction standards, and that this is not having a significant impact on costs. As with other HIPAA standards, most current entities will have a 2-year implementation period before compliance with the standards is required. Covered entities will develop their own implementation schedules, and may phase in various security measures over that time period.

## 3. Relationship to Privacy Standards

The publication of the final Privacy Rules (45 CFR parts 160 and 164) on December 28, 2000 in the **Federal Register** (65 FR 82462) and on August 14, 2002 (67 FR 53182) has affected the impact of this regulation significantly. Covered entities must implement the privacy standards by April 14, 2003 (April 14, 2004 for small health plans). The implementation of privacy standards reduces the cost of implementing the security standards in two significant areas.

First, we have made substantial efforts to ensure that the many requirements in

the security standards parallel those for privacy, and can easily be satisfied using the solutions for privacy. Administrative requirements like the need for written policies, responsible officers, and business associate agreements that are already required by the Privacy Rule can also serve to meet the security standards without significant additional cost. The analysis of data flows and data uses that covered entities are doing so as to comply with the Privacy Rule should also serve as the starting point for parallel analysis required by this final rule.

Second, it is likely that covered entities will meet a number of the requirements in the security standards through the implementation of the privacy requirements. For example, in order to comply with the Privacy Rule requirements to make reasonable efforts to limit the access of members of the work force to specified categories of protected health information, covered entities may implement some of the administrative, physical, and technical safeguards that the entity's risk analysis and assessment would require under the Security Rule. E-mail authentication procedures put into place for privacy protection may also meet the security standards, thereby eliminating the need for additional investments to meet these standards. As a result, covered entities that have moved forward in implementing the privacy standards are also implementing security measures at the same time. Since the proposed security standards proposed rule represents the most authoritative guidance now available on the nature of these standards, some entities have been using them to develop their security measures. Those entities should face minimal incremental costs in implementing the final version of these standards.

We are unable to quantify these overlaps, but we believe they may reduce the cost of implementing these security standards. The analysis provided to the HHS by the Gartner Group also stated that compliance with the Privacy Rule will have a moderate effect on the cost of compliance with the Security Rule, reducing it slightly.

## 4. Sensitivity to Security Concerns as a Result of September 11, 2001

In our discussions with the Gartner Group, they indicated that they saw little evidence of increased security awareness in health care organizations as a result of the events of September 11, 2001. However, a survey conducted by Phoenix Health Systems in the winter of 2002 showed that 65 percent of the respondents to the survey

(hospitals, payers, vendors, and clearinghouses) have moderately to greatly increased their attention on overall security. If these organizations have already made investments in security that meet some of the requirements of this rule, it will reduce their added costs of compliance. However, HHS can make no clear statement of the impact of this attention.

## D. Guiding Principles for Standard Selection

The implementation teams charged with designating standards under the statute have defined, with significant input from the health care industry, a set of common criteria for evaluating potential standards. These criteria are based on direct specifications in the HIPAA, the purpose of the law, and principles that support the regulatory philosophy set forth in the E.O. 12866 of September 30, 1993, and the Paperwork Reduction Act of 1995. In order to be designated as such, a standard should do the following:

- Improve the efficiency and effectiveness of the health care system by leading to cost reductions from or improvements in benefits from electronic health care transactions. This principle supports the regulatory goals of cost-effectiveness and avoidance of burden.
- Meet the needs of the health data standards user community, particularly health care providers, health plans, and health care clearinghouses. This principle supports the regulatory goal of cost-effectiveness.
- Be consistent and uniform with the other HIPAA standards (that is, their data element definitions and codes, and their privacy and security requirements) and, secondarily, with other private and public sector health data standards. This principle supports the regulatory goals of consistency and avoidance of incompatibility, and it establishes a performance objective for the standard.
- Have low additional development and implementation costs relative to the benefits of using the standard. This principle supports the regulatory goals of cost-effectiveness and avoidance of burden.
- Be supported by an ANSI-accredited standards developing organization or other private or public organization that would ensure continuity and efficient updating of the standard over time. This principle supports the regulatory goal of predictability.
- Have timely development, testing, implementation, and updating procedures to achieve administrative simplification benefits faster. This