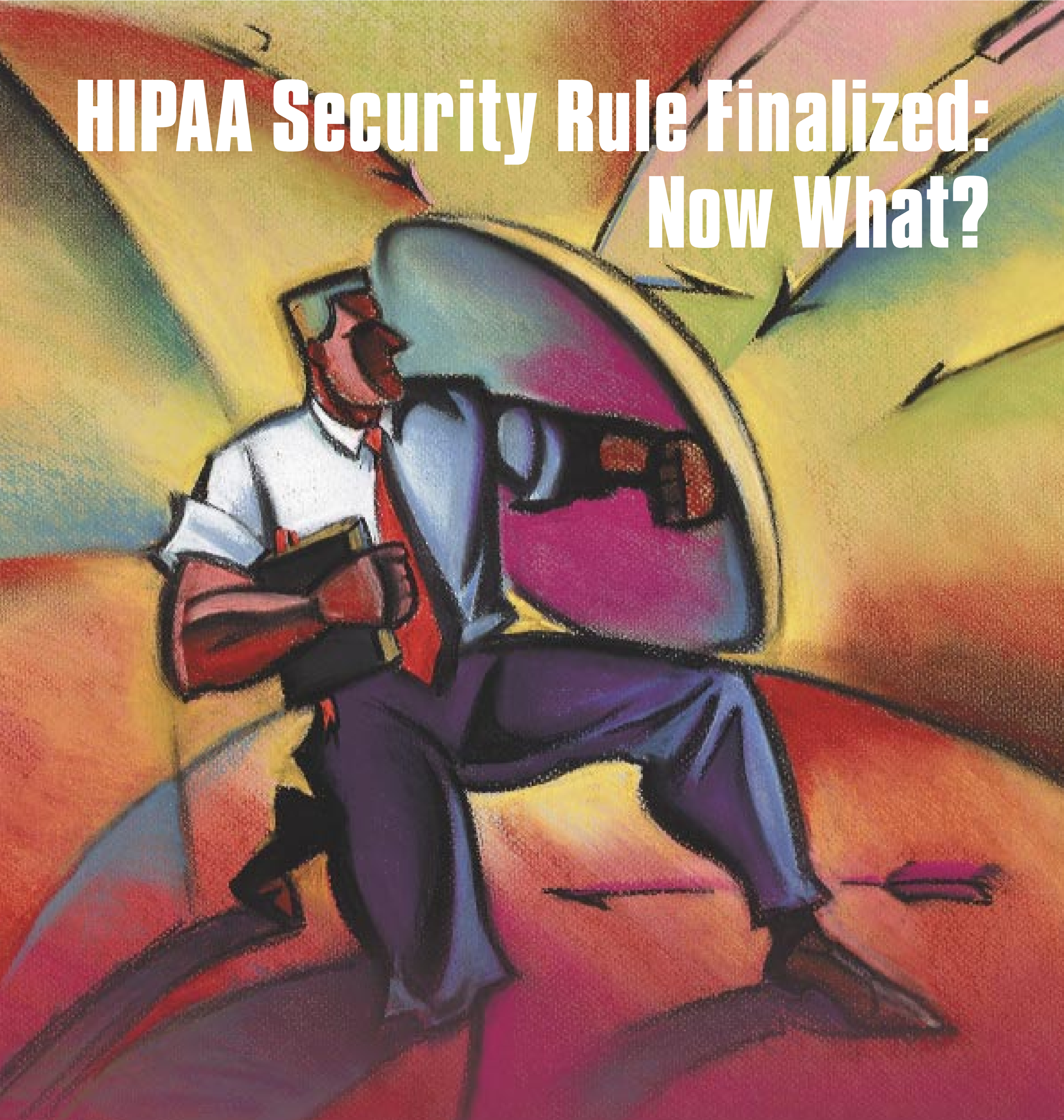
HIPAA Security Rule Finalized: Now What?



To shield themselves from potential headaches, healthcare organizations need to be targeting compliance as early as feasible.

BY ELISE CHIDLEY

After years of delay, a final rule designed to ensure the security of electronic protected health information (PHI) was published in the *Federal Register* on February 20.

A set of security standards for computerized PHI was first called for in 1996, when the Health Insurance Portability and Accountability Act (HIPAA) was passed. Luckily for hard-pressed healthcare organizations, the formulation of a final rule required a good deal of deliberation and fine-tuning.

Many in the healthcare industry are already familiar with much of the content of the finalized security rule—it was first published in 1998. According to Janet Hillock, chief privacy and security officer for HealthTrio, a provider of health and core business solutions for the managed care industry, "Although there are differences between the proposed and final rules, the basic requirements have been known for five years."

Now that the rule has been set in stone, healthcare organizations have been given two years to make the necessary changes. The effective date for compliance with security standards is April 21, 2005 (60 days plus 24 months after publication). Small health plans will have an additional year to comply.

This seems like a generous deadline now, but will healthcare organizations be up-to-speed by 2005, and how costly will the transformation be?

In a press release issued by Health and Human Services (HHS), Secretary Tommy G. Thompson optimistically predicted, "Overall, these national standards required under HIPAA will make it easier and less costly for the healthcare industry to process health claims and handle other transactions, while assuring patients that their information will remain secure and confidential."

However, many in the healthcare industry predict that implementation of the finalized security rule will require a significant investment of time, thought, and documentation—healthcare organizations should probably not become complacent about the seemingly safe distance of the deadline.

"The security rule is 'technology neutral' and does not require external solutions to meet most requirements," Hillock notes. "Organizations that cannot meet requirements internally should be looking for external assistance now. The process of purchasing and installing solutions can take time, and two years is not that far away."

The good news is that many of the differences between the final security rule and the proposed rule relate to making the standard more compatible with HIPAA's final privacy standards, which went into effect for most covered entities on April 14. According to the HHS, the two sets of standards use many of the same terms and definitions to make it easier for healthcare organizations to comply.

The finalized security rule is divided into three areas for compliance: administrative safeguards, physical safeguards, and technical safeguards.

Administrative safeguards make up 50% of the security rule's standards. These safeguards are largely concerned with establishing documented policies and procedures for daily operations; managing the conduct of employees who deal with electronic information; and managing the selection, development, and use of security controls. Basically, meeting the requirements for administrative safeguards involves assessing computer systems, training staff on procedures, preparing for the aftermath of hackers or catastrophic events, and developing contracts for business associates.

The good news is that many of the differences between the final security rule and the proposed rule relate to making the standard more compatible with HIPAA's final privacy standards.

The physical safeguards are designed to protect a healthcare organization's electronic information systems, as well as related buildings and equipment, from natural hazards, environmental hazards, and unauthorized intrusion. The measures include both administrative policies and physical controls. To comply with these safeguards, healthcare organizations must set procedures for facility-access control, workstation use and security, and electronic media reuse and disposal.

Technical safeguards include controlling staff computer log-in and log-off, monitoring access to patient information, and setting up a technical means of authenticating users. There are five final provisions in this area: access control, audit controls, integrity, person or entity authentication, and transmission security. They involve the following:

- Access control encompasses control of access by both people and software programs. Audit controls involve implementing the hardware, software, and/or procedural mechanisms to record and examine activity in information systems that contain or use electronic PHI.
- Integrity involves protecting electronic PHI from being meddled with or destroyed.
- Person or entity authentication entails procedures to verify that people or entities seeking access to PHI are who or what they claim to be.
- Transmission security, logically enough, involves implementing security measures to prevent unauthorized access to PHI while it is being electronically transmitted over a communications network.

A welcome feature of the final rule is its flexibility. According to Jeanette C. Schreiber, who chairs the HIPAA practice group at Wiggin & Dana LLP, "An unusually flexible approach to meeting the security standards is incorporated into the final regulations. Rather than requiring specific technical measures, the security rule takes a goal-oriented approach, establishing standards that all covered entities must meet but allowing the covered entity to choose, in many cases, whether or not certain implementation specifications apply."

Under technical safeguards, for example, healthcare organizations are encouraged to implement electronic procedures to encrypt and decrypt electronic PHI—but, encryption is not mandatory, only 'addressable.' Likewise, covered entities may or may not choose to implement automatic log-off—electronic procedures that terminate an electronic session after a predetermined time of inactivity.

For these 'addressable' implementation specifications, says Schreiber, the covered entity must address the reasonableness and appropriateness of the specification in relation to its own security framework, taking into consideration factors such as the cost of a particular security measure, the size of the covered entity, the complexity of the approach, and the nature and scope of potential security risks.

However, deciding how much security is enough may be a tough call for many covered entities. Schreiber advises trying to develop an understanding of the evolving industry standard for similar types of organizations when weighing how to implement the addressable standards.

According to Schreiber, the major challenge for healthcare organizations trying to meet the final security rule will be to translate the legal standards into technical solutions. Meeting this challenge, she says, will require "combined technical, legal, and administrative perspectives and expertise. As with other HIPAA compliance, a team effort is needed."

Many healthcare organizations will probably opt to reprogram an existing legacy system to meet the technical requirements of the security rule. Hillock cautions that reprogramming a legacy system can take as long as implementing a new one. "It's time-consuming, unreliable, and disruptive to the healthcare organization," she says.

According to Hillock, only three techniques have been shown to be effective with regard to making legacy systems compliant under HIPAA. They are as follows:

■ Replace

Administrative systems are one of a health plan's largest investments. Replacing whole systems that are currently managing business needs for the sake of legislation seems a steep price to pay, says Hillock, especially considering the organizational strain a system replacement engenders. The time required for implementation is also a major off-putting factor. According to Hillock, it's estimated that a midsized organization would require at least one year, perhaps two, to implement a new system. During the course of this implementation, other projects are put on hold, staff is bogged down with training, and overall business is disrupted, she warns.

■ Rewrite

This type of "upgrade" sounds like a pragmatic approach, but it is riddled with its own set of challenges, says Hillock. All such conversions can be expected to be over budget, time-consuming, and fraught with problems, especially if the legacy has been in use for some time. Through extensive analysis, an organization would have to determine where the current systems are noncompliant. Once the weak points are located, the systems would have to undergo an upgrade. In the end, this exhaustive reprogramming process could take up as much—or more—of an organization's time and money as purchasing a brand-new system, warns Hillock.

■ Wrap

There are new technologies that offer a low-cost, easy-to-implement alternative to installing new systems or reprogramming legacy systems—allowing an organization to safeguard and control proprietary information without having to alter the core administrative system. This new technology, which is external to an organization's core systems, effectively "wraps" legacy systems with a secure, HIPAA-compliant environment. Once in place, all transactions coming into or out of the organization's system, whether administrative—such as eligibility verification or claims submittal—or clinical—such as pharmacy orders or laboratory result lookup—are routed automatically through the wrapper. The wrapper then validates compliance with HIPAA security and authorization requirements. Acting strictly as a mediator, the wrapper solution leaves the back-end systems untouched. This solution is invisible to the user, although users will experience enhanced data access and availability with a wrapper in place. The final result is totally secure communications, Hillock promises.

If healthcare organizations turn to off-the-shelf solutions to help them comply with the new security rule, what should they be looking for?

According to Hillock, healthcare organizations should look for information systems—such as HealthTrio *connect*—that enable them to define user roles and determine what information each user can view, create, or modify. "This is fundamental to ensuring data security," she stresses.

Currently, many healthcare organizations do not have the ability to completely define a user and restrict his or her access to specific types of information. For example, many health-plan portal systems are not capable of allowing the office manager at a provider's office to access referrals, inquiries, eligibility, and claims data, while restricting access for other administrative staff to only certain items of eligibility data.

Most healthcare information systems with even the most basic security architecture have some level of restrictions with regard to particular display screens or patients. However, the level of control in most such systems alone is insufficient for the kinds of tight regulation over data access required by the security rule, Hillock believes.

She adds that to meet the security rule's requirements for audit trail functionality, audit trails must be able to track access at a high level of granularity—essentially, data element-level security. Healthcare organizations should look for information systems with an audit trail that captures and records all accesses, creations, updates, and edits for each piece of data within a patient record. Without the ability to secure data at the data-element level, many HIPAA-compliant systems will take healthcare organizations only part of the way toward achieving full security compliance, says Hillock.

Healthcare organizations should note that they are required to maintain all documentation (such as policies and procedures) required by the security rule for a period of six years from either the date of its creation or the date when it was last in effect—whichever is later. Such documentation must also be made available to those responsible for implementing related procedures. Finally, healthcare organizations must periodically review this documentation to update and revise it, if necessary.

What are the consequences of failure to comply with the new security rule? According to Schreiber, covered entities that fail to comply with the security regulations may be subject to the civil monetary penalties applicable to other HIPAA requirements.

The HIPAA statute sets a penalty of not more than $100 for each violation, subject to a calendar-year cap of $25,000 for all violations of an identical requirement or prohibition. The new interim final enforcement regulations (published April 17) begin the discussion of the process to be applied in imposing penalties, and future regulations will help define violations, Schreiber promises. She adds that covered entities also need to consider the possibility of private lawsuits being brought by individuals who are harmed by the entity's failure to comply.

How onerous will it be to comply with the new security rule? Only time will tell, but at least those healthcare organizations that have already worked hard to comply with HIPAA's privacy regulations can derive comfort from the fact that the security standards have been specifically designed to dovetail as much as possible with the language and requirements of the privacy rule.

— Elise Chidley is a freelance writer based in the United Kingdom.