

# STRATEGIES FOR COMPLYING WITH THE HIPAA SECURITY RULE

## ABSTRACT

*In response to the HIPAA privacy and security rules, organizations are taking steps to set up and clean up access controls, and explore possible changes to audit controls and termination procedures. They are facing the practical issues of implementing security policies that are compliant, efficient to administer, and not disruptive to users. Organizations are also setting up new users' system access according to role-based schemes and examining the ways they are terminating access for departing employees.*

**ANN PELLETIER, SUSAN A. BRESEE, AND JEFFREY R. HILL, MS**



Don't worry, spiders, I keep house casually.  
—Issa<sup>1</sup>

As the Health Insurance Portability and Accountability Act (HIPAA) privacy rule compliance deadline looms, covered entities (CEs) are in major housekeeping mode. Those who have kept house casually are confronting many a web to untangle.

Here is the scene. Organizations are scrambling to institute new policies and procedures, to revise existing practices, and to clear up noncompliant situations. Meanwhile, employees are coming and going as they always have, forcing entities to jostle between the pre- and post-HIPAA eras

when providing system access. How are organizations dealing with the practical issues of implementing security policies that are compliant, efficient to administer, and not disruptive to users? How are organizations setting up new users' system access according to role-oriented schemes? How are they terminating access for departing employees?

Early this year, we discussed the topic of HIPAA-compliant security with representatives of several entities, including a multispecialty provider network with 400-plus physicians serving California's East Bay communities, a for-profit regional health plan that services 40,000 enrolled members in the Pacific Northwest, and a university-affiliated physician group with approximately 700 providers in the state of Texas.

## KEYWORDS

*HIPAA    Security    Minimum necessary standard  
Role-based access control    Audit control    Termination procedures*

**Table 1. Terms Associated with HIPAA Privacy and Security Rules.**

Privacy	Security
Patient-centric	Covered entity-centric
Rights	Threats
Verbal, paper, electronic PHI	Electronically stored and transmitted PHI
Use and disclosure of PHI	Access to PHI
Standards	Safeguards

These organizations are all clients of our company, Global Works Systems, Inc. We provide value-added software applications, customizations, systems integration, and consulting services to healthcare practice management enterprises.

Our plan was to discuss HIPAA's security rule (still proposed at the time). Specifically, we intended to focus on the rule's call for access controls, audit controls, and termination procedures. Although we did cover all of these topics, clearly what was most on people's agendas was that area of overlap between HIPAA's privacy and security regulations, namely the implementation of access controls to ensure the minimum necessary standard outlined in the privacy rule. Audit controls and termination policies and procedures were on to-do lists, but most of the people we spoke with had not yet fully developed action plans for the proposed security rule requirements.

In this article, we report what steps organizations are taking to set up and clean up access controls, as well as share views on audit controls and termination procedures.

**Privacy and Security Compared and Contrasted**

HIPAA is a many-limbed creature whose extremities include standards for electronic transactions, the privacy of individually identifiable health information, security, and electronic signatures. Though publication of the final security rule lagged far behind the final privacy rule, the two sets of regulations were meant, according to the Department of Health and Human Services (HHS), to work in tandem.

Were we to play a game of free association with the HIPAA wise and weary using the words "privacy" and "security," we might generate something like the lists shown in Table 1.

A driving force of the privacy rule is the public's awareness of its right to privacy and its worry that, when it comes to individually identifiable healthcare information, that right is under threat. According to a California HealthCare Foundation survey, Internet and non-Internet users alike expressed that they are concerned or very concerned about breaches of privacy regarding their health information. The vast majority of online users worry that their health informa-

tion may be shared without their permission, that e-mails may be read by people other than to whom they were addressed, and that hackers may gain access to their health information.<sup>2</sup>

The privacy rule sets standards for the use and disclosure of a patient's health information, including what information a patient may, by right, obtain. The security rule details safeguards the covered entity must put in place in order to protect a

patient's privacy. The security rule's safeguards require organizations to attend to prevention of, preparation for, and response to both external and internal security threats. External threats include such things as the unauthorized interception of electronically transmitted data and viruses. Internal threats, believed to represent the greater incidence of risk, include violations of patient privacy caused by naïve or malicious employees.<sup>3</sup>

While the privacy rule deals with verbal, paper, and electronic forms of data, the security rule encompasses only electronically stored and transmitted protected health information (EPHI); thus it is the access and actions of a CE's systems users who are of central concern in the security rule.

**Minimum Necessary, Workforce Security, and Access Control Standards**

A chief protection of the privacy rule is the minimum necessary standard, which limits the extent to which protected health information (PHI) may be used, disclosed, or requested. This standard requires that access to PHI by employees of covered entities must be limited to the minimum necessary to do their jobs. The rule specifies that covered entities must "develop role-based access rules" to carry out this minimum necessary requirement.<sup>4</sup> Role-based access is the mapping of data access for a user or a class of users to only those functions, activities, and action codes that they need to perform their duties.

The security rule parallels the minimum necessary standard through both the access control standard (a technical safeguard) and the information access management standard (an administrative safeguard). In addressing access to EPHI, the access control standard focuses on the electronic information system, calling for limited access for software programs as well as members of the workforce. The information access standard requires a covered entity to "implement, if appropriate and reasonable to its situation, policies and procedures first to authorize a person to access electronic protected health information and then to actually establish such access."<sup>5</sup>

The security rule requires that CEs employ unique user identification to uphold the access control standard. Yet is this sufficient to also maintain the privacy rule's minimum necessary standard? Unique user ID will suffice only in a minimally staffed environment in which all system users need access to all EPHI. In this situation, the distinction between access according to user ID and role-based criteria collapse. All of the entities we work with, however, were too large for username/password control alone to suffice. All were earnestly working to support the minimum necessary standard through role-based access mapping.

**Setting Up Role-based Access**

According to the privacy rule, a covered entity must implement policies and procedures to identify all of the following:

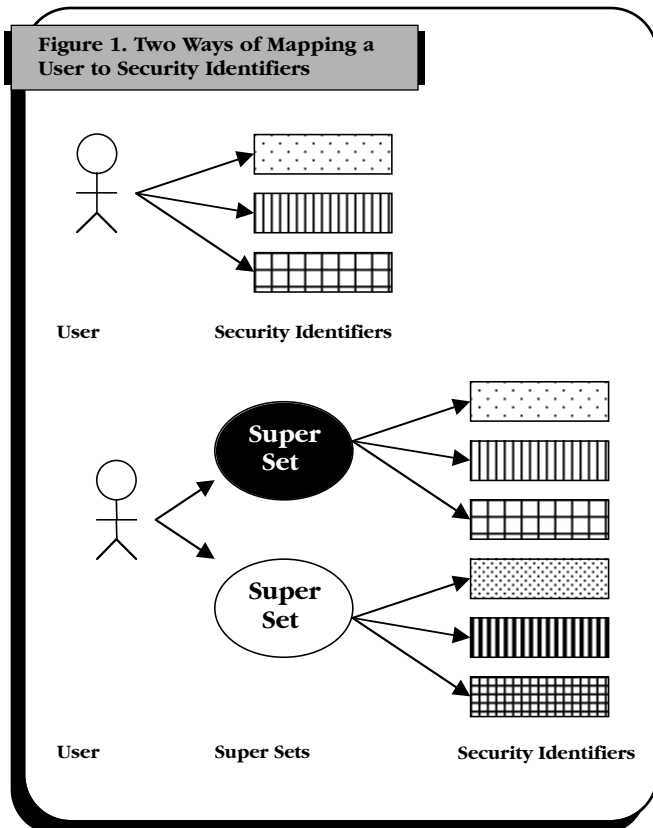
- The persons or classes of persons in the entity's workforce who need access to protected health information
- The category or categories of protected health information to which such persons or classes need access
- The conditions, as appropriate, that would apply to such access

Covered entities must also implement policies and procedures to limit access to only the identified persons, and only the identified protected health information.<sup>6</sup>

While the final security rule's access restrictions were made more general than in the proposed rule, HHS comments that the final version's "policies and procedures will enable entities to follow the Privacy Rule minimum necessary requirements, which provide when persons should have access to information."<sup>7</sup>

The organizations we spoke with use IDX® Systems for their practice management applications. IDX's security module supports role-based security access, allowing, in simplified terms, two methods of assigning the various necessary privileges to users. (See figure 1, Two Ways of Mapping a User to Security Identifiers.)

- User — Security Identifiers. The first method enables a direct mapping between a user and one or more security identifiers, each of which is attached to an application, function, activity, and/or action code. The relationship between user and category is generally one-to-many.
- User — Super Set(s) — Security Identifiers. The second method, available with later versions of IDX applications, includes the ability to create what we'll call "super sets." A super set is a set of security identifiers designed to support the access needs of a group of users. The relationship between user and super set can be many-to-one for more generalized roles, or few- or one-to-one for specialized roles. Although it is not possible with this type of configuration to manipulate the security identifiers for a particular user, it is possible to extend a user's access by assigning additional super sets.



All of the parties we interviewed had already had one of the above methods of security mapping — and thus the foundations for role-based access — in place for some time. In some cases, however, users were not necessarily assigned security with regards to their roles. And even when roles were considered, the minimum necessary standard was not. One client interviewee sums up the situation for all of the parties we spoke with, admitting, "If security isn't cleaned up, access will be considered inappropriately broad."

Security officers are now forced to untangle what one IS director describes as "years of haphazard processes of adding security." Why the mess? In many cases, IS staff habitually creates new super sets for new positions by copying an existing super set and then adding to it, without deleting any superfluous access. Similarly, when an employee changes departments, necessitating a different set of access, IS may retain the employee's existing access, adding to it whichever set or sets contain the newly needed security identifiers. Keep in mind that security categories can belong to any number of super sets, which means that IS people are faced with a seemingly infinite number of configurations.

In order to best map employees to the appropriate system access privileges, the IS staff needs to know who has access to what. Sounds simple enough, but this information is actually quite elusive. The security modules built into legacy systems typically pre-date HIPAA's minimum neces-

sary requirement; thus, security access has generally been based, not on roles per se, but on the nature of a user's transactions. And traditional security utilities do not offer the means of data analysis or enterprise-wide auditing, which require the merging and manipulation of information.

We have found that effective and efficient assessment of security configurations involves the extraction of key data from the transaction-based security module into a relational database. It's helpful to be able to report and query off data from a variety of points of view, for example:

- Security Identifier: which functions, activities, and action codes are associated with each security identifier; which super sets are mapped to each security identifier
- Super Set: what sets have been built in the system; each set's corresponding user and security identifier associations
- User: each user's super set or security identifier assignments

It's also helpful to be able to filter security setup data by properties, such as a single identifier, a group of identifiers, or by those security identifiers assigned to a particular department. This ability allows the security officer to break down cleanup into manageable tasks, and to present meaningful data to the appropriate people.

### **Cleaning Up**

What are the tasks of the cleanup crew? For many, it begins with a scouring of job descriptions. Some organizations have human resource initiatives in the works, requiring job descriptions to be rewritten to conform to role-based principles. Additionally, one physician group's security officer we spoke with has requested that, whenever possible, HR consolidate job descriptions. They have responded to this challenge by reducing the number of descriptions from 200 to 70.

Working from both job descriptions that emphasize roles and spell out access as well as a map of existing security assignments, IS people can clearly see the task at hand. The cleanup team can find redundancies of access sets, locate where security mapping needs vision, and note when altogether new sets of access must be built.

Once they clarify what needs cleaning up, security teams can begin the painstaking process of rebuilding security associations. The goal is to facilitate ongoing access management by creating as few super sets as possible while still holding to the minimum necessary standard. Interestingly, the efficiency of using super sets is more obvious for an organization with a large workforce, which may be quite easily split into groups with similar roles. A smaller organization whose employees have more specialized job functions with less overlap may find that the user to super set ratio is nearly one-to-one. Compare the organization with 500 system users and 70 super sets to the organization with 70 users, each tending toward a unique job description.

In either case, now armed with new, carefully considered sets of access, there are two routes to choose from:

- Flip-a-Switch. This is a feasible option for a smaller organization that can, say, reassign users to a fresh set of access and clear out the old over the course of a weekend. The IS project manager of a medical group with 150 system users plans to take this approach. Although he anticipates "some morning-after phone calls from frustrated users who cannot access certain functions," he and his team see this as an opportunity to evaluate whether people "are trying to access things they shouldn't get into."
- From-Now-On. With this two-step approach, all new hires and job changes within the organization are assigned to new super sets. Meanwhile, IS gradually transitions existing employees to new or redesigned super sets, one department (or other such division) at a time.

While everyone we spoke with was straining to comply with HIPAA standards, we also heard people agree that the security measures were a good idea. "Yes HIPAA has made us more aware of security," one party said, "but it's all normal security. It's just good practice." Another client told us of users inadvertently initiating processes that had nothing to do with their responsibilities. One user started the nightly batch process, a cascade of processes that significantly impacts system resources. Another user, in the midst of a check run process, accidentally kicked off the process that posts to accounts payable. So, compliance is certainly the primary motivating factor driving access cleanup, but there are other repercussions of slapdash access as well.

### **Termination Procedures**

As they are working to clean up and set up role-based access, our clients are also starting to establish timely termination procedures. "Hit or miss" was a typical response to the question, "What are your organization's current termination procedures?" Sometimes IS will receive notice of the need to terminate access, sometimes not.

The security rule's administrative safeguards include an addressable implementation specification that calls for procedures for terminating system access when no longer required. As with establishing compliant access protocols, effective termination procedures require cooperation between human resources or department heads and IS staff. IS must receive, and act on, termination notices in a timely fashion. Just as IS departments are now requiring signed, written requests from departments that specify what access an employee needs, they are also instituting forms that alert the IS department of the need to terminate access.

Establishing procedures and drawing up forms show the best of intentions, but experience shows that paper trails are not always foolproof. Our clients find it helpful to have

a means of checking their system for accounts that have not been accessed over a given period of time. This type of check can serve as a valuable tool in assessing the success of one's formal termination procedures. Account usage data can be used to identify vulnerabilities in the termination process and can serve as the starting point for developing a plan of action to strengthen procedures. When a review of system usage reveals that a particular account has not been accessed for some time, an investigation is in order. Is the employee in question still employed by the organization? Have the user's job responsibilities changed so that system access is no longer required?

Along with investigating the specific account, the security officer may wish to look for trends. How often is the IS security staff identifying inactive accounts? What tends to be the source of the lag? Is it a communication gap between HR and IS? Is a particular department delinquent in notifying the appropriate people about terminations? Is the IS staff having difficulty managing terminations in a timely manner? These questions form the basis for problem solving.

System usage data assists not only with HIPAA compliance but serves as a management tool as well. Unused accounts do not always represent unprocessed terminations. One security officer noted that such data revealed to managers that certain employees were neglecting some of their job responsibilities.

**Audit Controls**

The ability to monitor user behavior can serve to support both HIPAA's audit control standard as well as the organization's management objectives. The security rule requires organizations to establish audit controls that monitor their systems for security incidents and weaknesses. Security officers can benefit from reviewing:

- User activity — dates and times a user logged on or off the IDX system, from which terminal, and which application was engaged
- Improper logoffs — users who logged off improperly, potentially leaving a hung session, which, in turn, may leave a "back door" open

- Password changes — how often, if at all, users change their passwords

Security offers will also find it helpful to check for users who engage in a high number of simultaneous sessions. Not only does this information assist in monitoring user behavior, but also in obtaining the most cost-effective license agreements, as the number of concurrent sessions an organization may run is dependent on the terms of their contract with their practice management vendor.

**Future Directions**

What about organizations that employ additional systems? What about network-level access? How can security efforts be coordinated? Many people are voicing their frustration that there is no single tool on the market to help manage access and audit controls across systems. For now, people must set up and terminate access system by system and cobble together audit data from disparate sources.

One Global Works Systems client is eager to merge its practice management system's security setup data with like information from its other systems, extracting these data sets into a relational environment. We share the vision of a tool that goes beyond monitoring capabilities, enabling automated workflows for building and terminating security access across systems.

As organizations strive to clean up system access, they are finding that casual housekeeping must be relegated to being a practice of the past. Hopefully, in addition to meeting compliance, their efforts will foster better communication within the organization, better management of systems users, and, of course, a trusting relationship with patients.

**About the Authors**

Ann Pelletier is marketing editor for Global Works Systems, Inc.

Susan A. Bresee is a member of Global Works Systems' senior management team, working primarily in the area of business development.

Jeffrey R. Hill, MS, is a senior consultant for Global Works Systems, Inc.

References

<sup>1</sup>Hass, R., ed. *The Essential Haiku: Versions of Basbo, Buson, and Issa*. Hopewell, NJ: The Ecco Press, 1994, p. 153.

<sup>2</sup>Grimes-Gruckza, T., and Gratzner, C. *Ethics Survey of Consumer Attitudes About Health Web Sites*. Sponsored by California HealthCare Foundation and Internet Healthcare Coalition, 2000, p. 7.

<sup>3</sup>Gue, D. G. "The HIPAA Security Rule (NPRM): Overview." Phoenix Health Systems *HIPAA Advisory*, 2000-2003, p. 2.

<sup>4</sup>Department of Health and Human Services. "Standards for Privacy of Individually Identifiable Health; Final Rule." 45 CFR Subparts 160 and 164. 2000. *Federal Register*, 45, 60, 82746.

<sup>5</sup>Department of Health and Human Services. "Health Insurance Reform: Security Standards; Final Rule." 45 CFR Subparts 160, 162, and 164. 2003. *Federal Register*, 68, 34, 8358.

<sup>6</sup>See reference 4, 82544.

<sup>7</sup>See reference 5.