Access Controls: Striking the Right Balance

Save to myBoK

by Margret Amatayakul, MBA, RHIA, CHPS, FHIMSS

As healthcare organizations put the finishing touches on their HIPAA security compliance plans, many are finding that updating access controls is not easy. Clinicians often scoff at the word "control" in general and at "access control" in particular. Not all products are capable of supporting the level of access controls some organizations desire, and even when they do, creating the myriad roles to reflect user needs can be a daunting task. While this article can't provide a magic bullet, it does offer some practical advice on establishing the right level of access controls.

What the Regulations Say

To determine what access controls you need, start with the HIPAA regulations themselves. Section 164.312(a)(1) of the security rule indicates that a covered entity must (in accordance with §164.306 [general security rules]) "implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4)." Implementation specifications include unique user identification (required), emergency access procedures (required), automatic log-off (addressable), and encryption and decryption (addressable).

The reference to §164.308(a)(4), information access management, is important because it requires a covered entity to "implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part." Subpart E is the privacy rule. Within the privacy rule are two especially relevant requirements:

- §164.514, other requirements relating to uses and disclosures of protected health information, includes implementation specifications (§164.514(d)(2)) for minimum necessary uses of protected health information that state "a covered entity must identify those persons or classes of persons…in its workforce who need access to protected health information to carry out their duties; and for each such persons or class of persons, identify the category or categories of protected health information to which access is needed and any conditions appropriate to such access." Further, this section of the security rule notes that a "covered entity must make reasonable efforts to limit the access of such persons…to protected health information consistent with [the identification of need]."
- §164.502, uses and disclosures of protected health information, general rules (a)(2), states that minimum necessary does not apply to disclosures to or requests by a healthcare provider for treatment.

What the Regulations Mean

The references within the access control standard to the general security rules, the privacy minimum necessary general rules, and minimum necessary use rule mean that healthcare organizations must create access control policies and procedures consistent with their risk analysis (from the general security rules) and with their minimum necessary policies (from the privacy rule).

It would be simple to let it go at that. After all, privacy compliance was required nearly two years ago, so organizations should have minimum necessary use policies that clearly establish classes of persons, categories, and conditions for access that can be directly applied to their information systems. Unfortunately, most organizations' minimum necessary use policies and procedures were focused on paper-based record systems with the hope that the security rule would further elaborate and establish what is needed for electronic systems. Further, most clinicians will quickly point to the fact that minimum necessary does not apply to treatment. As with all of the HIPAA standards, however, interpretation of these standards varies by person or group.

When Reality Sets In

It is clear from the rules that there are several things an organization needs to consider in constructing its access controls. There is also leeway that some organizations do not appear to be considering.

The meaning of a treatment relationship. Most organizations define a treatment relationship as one in which a clinician has direct responsibility for a patient's care. The corollary would be if a clinician does not have a direct responsibility the clinician should not have access (e.g., a patient who is not on the nursing unit for which a nurse has been assigned or a patient to whom a physician is not the provider or a consultant). While this is the generally held meaning, most healthcare organizations are experiencing push back, especially from physicians. They believe that there is always the potential for a treatment relationship with patients in hospitals, such as in an emergency. An organization should point out that such is the exact reason for the security rule's implementation specification for emergency access procedures. Unfortunately, most organizations' information systems do not yet have the capability to readily provide such procedures, and many clinicians do not trust that instantaneous access will truly be available when needed.

One way to approach this is to recognize the issue, document that steps are being taken to achieve strong access controls that afford appropriate emergency access, and then contact your vendor to determine what regulatory upgrades they are planning and when you can expect delivery. If the vendor is not as responsive as desired, evaluate third-party software. This is where your risk analysis is critical. If the third-party software will work with your present information system and is generally within your budget, then steps should be taken to acquire and implement it. However, if there is no software that works reasonably well for a reasonable price, document this, and plan to upgrade existing access controls to the extent possible. This may be less than what you initially thought you should do, but your due diligence should support your decision.

Interpretation of classes of persons, categories of need, and conditions for access. General interpretation is that this means role-based access controls, with an elaborate classification, categorization, and logic to support conditions.

Here again, a reasonable approach should be taken. Start with a basic process and assess the risk for not having stricter controls. If the risk is more than what the organization is willing to accept, tighten the process and reassess the risk. Too often organizations start out assuming the tightest structure. Starting at the baseline, however, allows implementation in stages.

Establishing procedures for emergency access. Once again, general interpretation has commonly meant "break-the-glass" controls within an information system. Such a practice allows access after a second password or rationale for need is entered by the user who is not ordinarily authorized access to the patient or data. This is usually accompanied by a special audit trail potentially to a supervisor, attending physician, or compliance officer. If access controls are not originally set properly, this procedure can be a nightmare to administer.

In approaching this consideration, it should be recognized that the security rule does not require any special type of procedure, only a procedure. It is conceivable that such access could be granted in a less onerous manner.

Access controls for software programs. In addition to access controls to prevent unauthorized use and disclosure with respect to persons, this requirement refers to the ability for one software program to access data from another. For example, can a data-abstracting program access all patients' records or only certain records as may be specified? Will charge capture systems capture every charge, even for sensitive tests or procedures?

In most cases, the organization has already considered these factors. If so, they should be documented as the approach to compliance. If not, consider the systems' information flow and ensure there is a rationale for the exchange of data. It would certainly be within an organization's treatment, payment, and operations uses to capture charges for all tests and procedures. However, a thorough review of the information flow may reveal that information is flowing more than necessary. In this case, steps should be taken to restrict the flow as necessary.

Exercising the Options	
Risk Mitigation Option	**NIST Definition**
Risk assumption	Accept potential risk and continue operating the IT system or implement controls to lower risk to an acceptable level.
Risk avoidance	Avoid the risk by eliminating the risk cause and/or consequence

Risk limitation	Limit the risk by implementing controls that minimize the adverse impact of a threat's exercising a vulnerability
Risk planning	Manage risk by developing a risk mitigation plan that prioritizes, implements, and maintains controls
Research and acknowledgment	Lower the risk of loss by acknowledging the vulnerability or flaw and researching controls to correct it
Risk transference	Transfer the risk by using other options to compensate for the loss, such as purchasing insurance

Source: Stoneburner, Goguen, and Feringa. "Risk Management Guide for Information Technology Systems."

NIST to the Rescue

The National Institute for Standards and Technology (NIST) is the body within the federal government that establishes security standards for federal information systems. NIST is referenced in the HIPAA security rule as a resource. NIST includes among its documents "Risk Management Guide for Information Technology Systems." This document provides excellent information on how to conduct a risk analysis. In addition, it describes several risk mitigation options an organization might consider as it plans its security strategies.

It is important to recognize that risk planning and research and acknowledgment are among the options. This means that so long as you document known vulnerabilities—such as not yet having automated emergency access procedures—and indicate what you are doing instead (such as using a special password) and how you are planning to improve the security measures in the future, you would be consistent with NIST's advice on risk mitigation. This does not mean you should disregard the need for stronger controls or that you can choose to address them whenever you want. But it does indicate that you are actively engaged in attempting to achieve a better solution.

Reference

Stoneburner, Gary, Alice Goguen, and Alexis Feringa. "Risk Management Guide for Information Technology Systems." Special publication 800-30. National Institute of Standards and Technology, 2002. Available online at http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

Margret Amatayakul *(margretcpr@aol.com) is president of Margret\A Consulting, LLC, an independent consulting firm based in Schaumburg, IL.*

Article citation:
Amatayakul, Margret. "Access Controls: Striking the Right Balance." *Journal of AHIMA* 76, no.1 (January 2005): 56-57.