Translating the Language of Security (HIPAA on the Job)

by Margret Amatayakul, RHIA, CHPS, FHIMSS

There were no big surprises in the final security rule. As promised, it has been reconciled with the privacy rule and most redundancies were removed. The security rule addresses only electronic protected health information (ePHI), though we must not forget the privacy rule's "mini-security rule" (the requirement for administrative, physical, and technical safeguards to protect the privacy of protected health information (Sec. 164.530[c][1]).

The final security rule emphasizes risk analysis to determine how to address the requirements. Possibly the only surprise is the "required" and "addressable" designations for implementation specifications. This treatment of how to implement the standards provides even more scalability, flexibility, and technical neutrality than the proposed rule. Coupled with the fact that the term "reasonable" appears 57 times throughout the 49 pages of preamble and standard, the final rule is even less black and white than the proposed rule, something IT professionals will find even more troubling.

Mission Impossible?

To develop security regulations applicable to every form of covered entity—from a small dentist office to a huge, multi-state health plan—the government had to modify its primary source of information security principles (the Department of Defense) for a vastly different industry. Then it attempted to use a regulation predicated on mainframe technology, update it, and make it last for many years.

This article aims to translate parts of the final security standards into principles that may afford more definitive best practices for healthcare today.

What Does "Best" Really Mean?

The term "best practice" is a good place to start. It should be understood that "best" does not mean "most," as in most expensive or most organizations practice this way. A best practice is a way to do something that is most efficient and effective.

For example, if a hospital is having difficulty getting users to save documents to a network rather than the hard drive on their workstations, a best practice may be to name the network drive "C," which is typically the hard drive, and rename the hard drive something else.

Get the Terms Straight

Required and Addressable

The terms "required" and "addressable" are also critical to understand. Just because they are a pair of terms does not mean that the opposite of required is "not required." Addressable means that the proposed way to implement a standard needs to be evaluated for the environment. If the proposed implementation specification makes sense, it should be adopted. If there is a better alternative, the alternative should be justified and adopted. If the implementation is not applicable, this should be described.

"Addressable" only applies to implementation specifications. All standards are required. For example, the standard on transmission security has two implementation specifications: integrity controls and encryption, both of which are addressable. This does not mean that a covered entity does not need to secure its transmission of PHI; it just means that it needs to describe how it will implement integrity controls and encryption when transmitting PHI.

Risk Analysis and Gap Analysis

Another pair of terms to distinguish is "risk analysis" and "gap analysis." The final rule does not use the term gap analysis, but many organizations conducted a gap analysis for privacy, security, and transactions when the privacy rule was published. The gap analysis identified the elements that may have been missing in the organization, such as the notice of privacy practices, audit trails for security, or a translator to create X12N transactions.

Very few organizations conducted an actual risk analysis in which each gap in security (known as a vulnerability) is evaluated in light of potential threats to determine level of risk. For example, not having an audit trail is a vulnerability. The threat is inappropriate access that is difficult to prove.

Risk is described in the final rule as a combination of the probability the threat will occur and the criticality the threat poses to the organization. (See "Assessing Probability, Criticality of Potential Risks to ePHI, " below.) Thus, the risk of not having audit trails is a violation of the regulation and the potential inability to impose sanctions for breach of confidentiality or prove that access occurred or was a violation.

A qualitative risk analysis describes probability and criticality by ratings such as high, medium, and low. This is a good way to start the process, but obviously does not provide any measure of return on investment in security controls. In an environment where budgets are tight and the rule is gray, it may be worth the effort to be more quantitative.

There are several degrees of quantification. A simple quantification might assign a numeric value to the combination of probability and criticality. This helps to prioritize remediation of risks.

A cost-based risk analysis may be calculated by estimating loss (for example, the cost of fines, a lawsuit, or public relations effort to regain consumer confidence) and comparing it to the cost of remediation (for example, purchasing a new system, recovering data, or ongoing maintenance). Such an estimate, however, does not consider the probability that the threat would occur. For example, a lawsuit may cost $1 million and remediation costs $100,000. But if the CEO believes the likelihood of a lawsuit is one in a million, then he or she could argue that any cost to remediate more than $1 is too much.

Security experts use an annualized loss expectancy calculation that factors in the probability of the threat and its criticality. This calculation must be performed with relatively accurate information for it to be worth the effort, but it provides a much more realistic picture and justification for security controls.

Information Access Management, Work Force Security as Complements

The information access management and work force security standards in the final rule may appear to include some redundancy and may suggest some missing elements or relaxed requirements. The standards are complementary and each has an important, unique function. Best practice suggests strengthening controls, potentially through use of a centralized suite of controls.

Information access management includes implementation specifications on authorization, establishment, and modification of access privileges. Establishing access for a new or transferred member of the work force is often less than timely and sometimes results in decentralizing the function at the department level.

Note that the duties of access authorization and establishment should be separated and taken very seriously. In fact, the issue of access may be the largest area of potential risk that the healthcare industry has not acknowledged because in the past, many information systems were not mission-critical and access controls were generally weak.

For example, a manager who authorizes Mary's access "just like" Sharon's is not taking care to ensure that Mary really needs the same access. A harried employee in IT who takes John's word for the fact that he needs his old access reinstated is succumbing to social engineering—an increasingly common technique to gain inappropriate access. Administration that does not support tighter controls is operating under the mistaken impression that security breaches won't happen at their facility.

Complementary to access authorization and establishment are work force security standards. These include authorization/supervision (a holdover from mainframe days), clearance checks (which should be done before access authorization), and termination procedures (for which managers should be held at least equally if not more accountable than for access authorization).

A Closer Look at Access Controls, Authentication

The final security rule provides an additional challenge in the removal of implementation specifications relating to types of access controls. No longer are user-based, role-based, or context-based access controls identified. Some infer, therefore, that these are not necessary. However, in keeping with the intent to make the rule timeless, these options were simply not enumerated because there are currently other forms of access controls and new forms may yet be invented. The minimum necessary use requirement in the privacy rule, however, makes it very clear that classes of workers needing access, categories of PHI to which access is needed, and conditions appropriate to such access need to be defined. Such access classes, categories, and conditions require, at a minimum, what is typically called role-based access controls, if not context-based controls.

While access controls establish the means to achieve minimum necessary use, emergency access procedures, automatic logoff, and encryption/decryption are included in this standard as well.

The rule defines emergency access procedures as "procedures for obtaining necessary ePHI during an emergency." Considering that there are emergency mode procedures under contingency planning, this definition seems either redundant or inconsistent with the commonly considered meaning of emergency access procedures as "break-the-glass" functionality. Break-the-glass (which draws its name from breaking the glass to pull a fire alarm) refers to a quick means for a person who does not have access privileges to certain information to gain access when necessary. Typically, a special audit trail is created to monitor such access.

Access controls should be established with sufficient rules to minimize the number of times break-the-glass needs to occur. That emergency mode procedures are a required implementation specification suggests that strong access controls are expected.

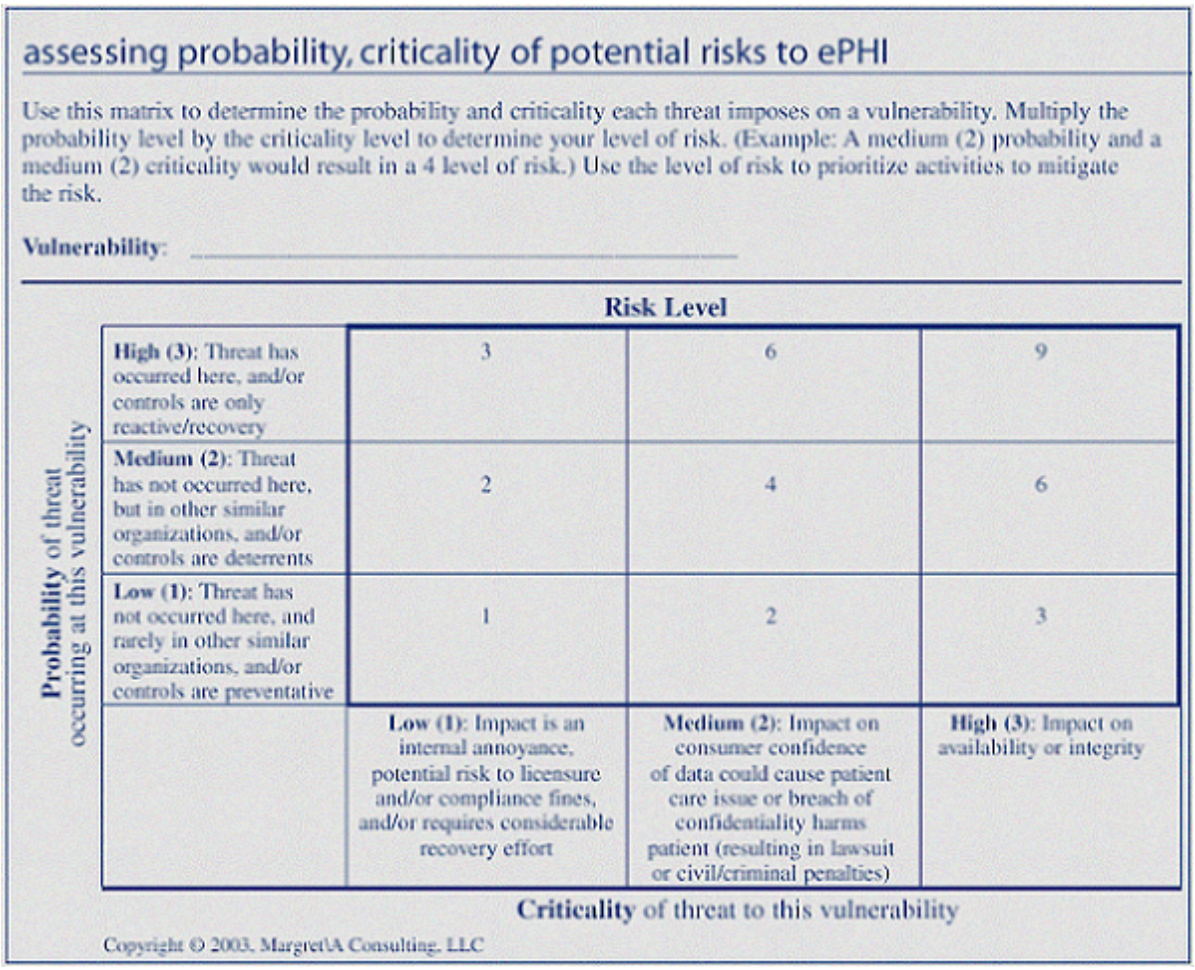
Automatic logoff is designated as an addressable implementation specification of access controls—so that the environment can help determine whether this is needed and the timing for which the logoff should be set. For example, automatic logoff could be set for a full day in the office of a small physician's practice that is inaccessible by the public, in comparison to a few minutes for a hospital's registration area.

Encryption/decryption is also addressable in the access control standard. The final rule supposedly does not distinguish controls for data at rest (that is, within an information system) from data en route (that is, transmitted through a network). However, there is a separate standard for transmission security with its own addressable implementation specification for encryption. This suggests that the intent is for encryption to be employed in both cases as appropriate. It is certainly greater protection than typically afforded data at rest. But perhaps this is a case of the government anticipating the future, where data in mobile computing devices should be encrypted because the device itself moves and is prone to loss.

Finally, authentication refers to the mechanism to prove the person seeking access is the one claimed. Obviously, it relates very closely to access. The healthcare industry has usually managed the various components of access separately. Best practice, however, would suggest stronger overall management and centralization. A single suite of products may be able to manage authorization, establishment, termination, and adherence to password policy. Single login, with or without biometrics, may be another suite of products to manage this process.

HIPAA Lessons Learned

This article addresses only a portion of the security controls required in the final rule. Healthcare organizations, however, should consider lessons learned from the privacy rule. Security controls are generally costlier to purchase, implement, and manage on an ongoing basis than privacy controls. The requirement for security risk analysis was placed first in the rule to emphasize its importance and prioritization. It is the key to budgeting for the rest of security and should be done well in advance of when the controls need to be implemented, tested, trained on, and revised as necessary prior to the compliance date of April 20, 2005.



assessing probability, criticality of potential risks to ePHI

Use this matrix to determine the probability and criticality each threat imposes on a vulnerability. Multiply the probability level by the criticality level to determine your level of risk. (Example: A medium (2) probability and a medium (2) criticality would result in a 4 level of risk.) Use the level of risk to prioritize activities to mitigate the risk.

Vulnerability: _____

Risk Level

Probability of threat occurring at this vulnerability	**Low (1)**: Impact is an internal annoyance, potential risk to licensure and/or compliance fines, and/or requires considerable recovery effort	**Medium (2)**: Impact on consumer confidence of data could cause patient care issue or breach of confidentiality harms patient (resulting in lawsuit or civil/criminal penalties)	**High (3)**: Impact on availability or integrity
High (3): Threat has occurred here, and/or controls are only reactive/recovery	3	6	9
Medium (2): Threat has not occurred here, but in other similar organizations, and/or controls are deterrents	2	4	6
Low (1): Threat has not occurred here, and rarely in other similar organizations, and/or controls are preventative	1	2	3

Criticality of threat to this vulnerability

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

Article citation:
Amatayakul, Margret. "Translating the Language of Security (HIPAA on the Job series)." *Journal of AHIMA* 74, no.6 (June 2003): 16A-D.