Kick Starting the Security Risk Analysis

by Margret Amatayakul, MBA, RHIA, CHPS, FHIMSS

Many covered entities are just now starting to approach the compliance aspects of the HIPAA security rule. Why discuss "compliance aspects" and not standards or controls, as we did when preparing for the privacy rule? Privacy and security are long-standing concepts to healthcare, but security might be considered older than privacy with respect to HIPAA, and organizations are likely to have significant security controls already in place. While new controls may be needed to address some HIPAA standards, many organizations are finding that the weakest aspect of security in healthcare is documenting existing controls and the ways in which they reduce risk.

The HIPAA privacy rule imposed a number of new processes and procedures and required considerable information flow analysis. Take away "health" in HIPAA, however, and the security rule is really no different than the international security standard (ISO/IEC 17799), standards for securing federal government information systems (published by the National Institute of Standards and Technology and Centers for Medicare and Medicaid Services for its contractors), security required under the Gramm-Leach-Bliley Act for the financial services industry, or any other security measures adopted for good business practices. One of the key differences for covered entities with respect to the HIPAA security rule, however, is risk analysis.

The security rule requires a covered entity to undertake "an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity."[1] In its general requirements, the security rule notes that "in deciding which security measures to use, a covered entity must take into account … [its] size, complexity, and capabilities; technical infrastructure …; costs of security measures; [and] the probability and criticality of potential risks to electronic protected health information."[2]

Risk Analysis Defined

A risk analysis, then, is a process whereby an entity identifies not only its vulnerabilities, as it did in its preparations for compliance with the privacy rule, but also identifies threats in its environment and determines the likelihood that a threat would exploit a vulnerability and cause harm. Determining this risk keeps costs down by recognizing that there is no such thing as total security and that the vulnerabilities most important to address are those that are most likely to be attacked. It further supports compliance because the justification for the selection of controls is reflected in the documentation of the risk analysis.

Identifying Threats

While identifying vulnerabilities is a matter of due diligence, identifying threats is new for healthcare, and it's not easy. It may help to consider the components of a threat. Typically, threats include agents, targets, and events, as illustrated in the figure "Threats in Relation to Risk".

Threats in Relation to Risk

Threats			Vulnerabilities	Risk	Controls	Residual Risk
Agents	Targets	Events	Gaps in administrative, physical, and technical safeguards		Policies, procedures, training, physical structures, technical controls	
Unauthorized access	Confidentiality	Wrongful disclosure and privacy violation				
Modification or destruction of data	Integrity	Erroneous information and medical errors				
Denial of service	Availability	Lack of critical informaion for patient				

		care, productivity issues, recovery costs				
Repudiation	Accountability	False claims or lack of evidence				

When HIPAA defines risk it means identifying threats that may exploit vulnerabilities. This helps prioritize controls that reduce that risk and makes it clear what level of risk remains even with the controls in place.

- **Agents** are the ways in which people or natural acts initiate a threat, whether accidental, deliberate, or the result of a natural act.
- **Targets** are the focus of the threat. HIPAA identifies three targets: confidentiality, data integrity, and availability; many security experts add a fourth—accountability.
- **Events** are the resultant harm from agents targeting vulnerabilities.

In identifying the probability that a threat would exploit a vulnerability, consideration should be given to whether a vulnerability has been threatened previously, how frequently the threat occurs, if the threat source has a high degree of knowledge and motivation, and what controls exist.

The other part of the risk equation is criticality of impact. If a threat were to exploit a vulnerability, what harm would it do? Will it affect patient care, cause a breach of confidentiality, result in a complaint or lawsuit, reduce productivity, cause loss of revenue, or raise a public relations issue?

Conducting the Risk Analysis

Different security experts may use slightly different approaches to risk analysis. Following are the most common steps in a risk analysis:

1. **Convene a group** to conduct the risk analysis. Be sure to include representatives of all parties concerned, including users. Users can both help to identify actual threats they see everyday and help achieve buy-in for new controls.
2. **Understand executive management's risk position.** The February 2004 "HIPAA on the Job" column provides tips on securing executive support for security.
3. **Take an inventory** of security policies and procedures, the physical environment, current information systems applications, medical devices, network, operating system, and hardware.
4. Using the inventory, **identify security gaps,** or vulnerabilities, in the policies and procedures, physical environment, current information systems applications, medical devices, network, operating system, and hardware. It may be helpful to summarize the vulnerabilities with respect to each HIPAA security standard.
5. **Identify threats** that might exploit the vulnerabilities. Be realistic and as precise as possible. The more you are able to do so, the better your rationale will be for recommending appropriate controls.
6. **Determine the probability and criticality** of threats exploiting vulnerabilities. A scoring tool, such as the "Risk Scoring Scale" expresses the level of risk as a numerical value, allowing for easy ranking.

Risk Scoring Scale				
Probability of Occurrence	High	3	6	9
	Medium	2	4	6
	Low	1	2	3
		Low	Medium	High
		Criticality of Impact		
© 2004, Margret\A Consulting, LLC				

A risk scoring scale helps achieve objectivity in determining the probability that a threat will exploit a vulnerability and have a critical impact. The higher the score, the greater the overall risk.

7. **Propose controls** for each area of risk. If executive management is risk averse, you may identify new controls for every area of risk. If executive management is more risk tolerant, you may identify new controls only for areas with high to medium levels of risk.
8. **Estimate the level of residual risk** that exists after the recommended controls are put into place. Although HIPAA does not require an estimation of residual risk, this is extremely helpful to executives in evaluating the budget associated with the controls you recommend. For example, if they find that audit controls you recommend only reduce the level of risk from 6 to 4, they may decide to beef up policy enforcement that might have the same effect for less money. Alternatively, if you recommend improved training for users on strong passwords and only reduce risk from 6 to 4 for authentication, executive management may ask if risk can be lowered further with technical control that force strong password creation. It is important to understand executive management's risk position prior to recommending controls so that you are most likely to recommend ones appropriate to their risk profile.
9. **Document** everything associated with the risk analysis. Even if you determine that one or more of the standards have very low risk in your environment, it is important to document how you know the risk is low.
10. **Plan for ongoing risk management,** so that changes in the environment, in systems, or in any other factor are identified and new threats and vulnerabilities assessed. Just as with privacy, security is an ongoing effort.

Less Than a Year Away

The compliance deadline for security is April 21, 2005. Most organizations are estimating that it will take at least two to four months to conduct their inventories. Some controls will be relatively easy to implement, but others may require advance budgeting, a formal selection process, scheduled installation, and training for use.

Perhaps the biggest issue is that some healthcare information systems vendors do not address all of the necessary controls or do not address them at the level an organization's risk score would require. Just as with Y2K, it may be necessary to contact the vendor and determine what solution will be available, when, and what resources it may require.

Notes

1. "Security Standards Final Rule." 45 CFR Part 164. *Federal Register* 68, no. 34 (2003): 8377. Available online at www.cms.hhs.gov/hipaa/hipaa2/regulations/security/03-3877.pdf
2. Ibid, 8376.

References

Amatayakul, Margret. "Finding Quality HIPAA Security Resources." *Journal of AHIMA* 75, no. 1 (2004): 58–59.

Amatayakul, Margret. "The HIPAA Security Shopping List." *Journal of AHIMA* 75, no. 5 (2004): 44–45.

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

Article citation:
Amatayakul, Margret. "Kick Starting the Security Risk Analysis." *Journal of AHIMA* 75, no.7 (July-August 2004): 46-47.