# Putting the Finishing Touches to Security: Are You Ready?

Save to myBoK

*by Margret Amatayakul, MBA, RHIA, CHPS, FHIMSS*

Many covered entities have enhanced their security measures over the last several years in preparation for the HIPAA security rule compliance deadline. In the March issue, Tom Walsh provided a readiness checklist to ensure your organization had the necessary processes in place (See "The 26.2-mile Security Rule"). The last step should be to check that the processes are being followed and achieving results.

To do so, focus on the most vulnerable areas and test that new policies and procedures actually work. Verify that those that have been in place are being followed. Many of the items in the checklist provided here are not new, but that's the point—whether addressed during preparation for the HIPAA privacy compliance regulations or as part of good business practices, organizations must check that all is well or mitigate risk in time for the security compliance deadline.

## Readiness Process

The information privacy officer and information security officer (if not the same person) should conduct a readiness review together. Most security incidents will result in a breach of confidentiality. Even though the Centers for Medicare and Medicaid Services (CMS) have jurisdiction over security rule enforcement, most HIPAA complaints will very likely be directed to the Office for Civil Rights (OCR) because they look like privacy issues even though they may stem from weak security. In addition, the notice of privacy practices refers complainants to OCR. There is no requirement for such complainants to distinguish between lax security measures or privacy issues as the cause of a breach of confidentiality. However, it is conceivable that complaints that appear to arise from security matters will be turned over to CMS or investigated by both OCR and CMS. As a result, it is a good idea for a covered entity to approach final preparations for compliance with the HIPAA security rule from a similar perspective.

## Readiness Checklist

Use the readiness checklist below as a final walkthrough prior to April 20, 2005. This is not a technical assessment but rather a check to make sure that workarounds are not being used to avoid or circumvent technical controls. A large percentage of security incidents are the result of human error, not machine failure. This does not mean that technical controls should be ignored, but that such checks alone are insufficient.

The checklist looks at specific vulnerabilities known to be common areas of concern. If you have identified additional vulnerabilities, add them to your list. Describe the status of each area on the date of the walkthrough, which should ideally be conducted a few weeks prior to the compliance deadline date. Record recommendations for mitigating any risk that appears high and indicate a follow-up date.

| **HIPAA Security Checklist** | | | |
|---|---|---|---|
| Date: Performed by: | | | |
| **Vulnerability** | **Status** | **Recommendation** | **Followup** |
| 1. Has a security risk analysis been performed and documented, with dates planned for subsequent evaluation? | | | |
| 2. Is there evidence that sanction policies for privacy and security violations are followed consistently? | | | |
| 3. Does information system activity review provide documentary evidence of analysis and action taken as appropriate? | | | |
| 4. Have work force clearance procedures been addressed for all forms of work force members, especially temporary staff? | | | |

| | | | |
|---|---|---|---|
| 5. Is there a clear process for termination of access for all members of the work force, and is the process carried out as specified? | | | |
| 6. Is there separation of responsibility for authorizing access and establishing access? | | | |
| 7. Is authorization of access privileges retained and retrievable should there be an investigation into how an individual was authorized access? | | | |
| 8. When a member of the work force changes job responsibilities, is appropriate modification to access privileges made? | | | |
| 9. What evidence is there that the organization provides security awareness and reminders? Can all such evidence be retrieved easily in the event of an investigation? | | | |
| 10. Do all members of the work force know how to create strong passwords, and is there evidence that strong passwords are used? | | | |
| 11. Do all members of the work force understand what constitutes a reportable security incident? Does the organization distinguish between security events and security incidents, and if so, clearly describes how each is handled? | | | |
| 12. Is there documentary evidence that back-up procedures are followed, including testing that backups can be restored (not just that they have been restored the last time there was a need)? | | | |
| 13. Are there contingency plans in place and widely available to all who need to know? | | | |
| 14. Are contingency plans consistent with the level of protection needed? For example, if an organization has a hybrid record system, is there full redundancy for the electronic portion of the hybrid record? | | | |
| 15. Have business associate agreements been revised to reflect security requirements, including the need for business associates to report security incidents they or their agents encounter to the covered entity? | | | |
| 16. Is there a facility security plan that addresses not only data center security but also physical security in all other parts of the physical infrastructure? | | | |
| 17. Are documents containing personal health information shredded or otherwise appropriately discarded? | | | |
| 18. Are media reuse policies followed? Are media to be reused or discarded stored in an appropriate location and accounted for? | | | |
| 19. Are handheld and other portable devices tracked and protected according to policy? For example, is cache memory deleted when out of range of wireless? | | | |
| 20. Are access controls consistent with minimum necessary use policies? Does every member of the work force use a unique user ID? | | | |
| 21. Are emergency access procedures implemented? | | | |
| 22. Is automatic log-off set appropriately for the location and use of workstations? | | | |
| 23. Is there a means to proactively analyze audit trail data in a meaningful and efficient manner? | | | |
| 24. Are authentication measures consistent with the risk associated with each form of access? For example, if remote access is deemed riskier than on-site access, is two-tier authentication used? | | | |
| 25. Has the need for encryption of data at rest or during transmission been evaluated and appropriate measures taken? For example, is a Web portal used instead of e-mail? | | | |

## Readiness Documentation

The results of the final walkthrough should be documented. Whether you use the checklist provided here or you refer back to an assessment that was performed, the final check documents that plans have been implemented. The final checklist provides a baseline for compliance for identified vulnerabilities. From this point forward, continued evaluation is necessary (and required by HIPAA) in order to determine if any changes need to be made based on new risks that may arise in the environment, such as new threats, updated technology, or even continuation of workarounds.

In HIM, we're fond of saying that "the record defends its friends." In security, documentation provides evidence of ongoing monitoring. The final check and its documentation serve to suggest where continual monitoring is needed, when an adjustment needs to be made in triggers for special review, or where residual risk remains high and plans need to be made to lower the risk.

This month we feature the final "HIPAA on the Job" column. With the implementation dates of the privacy and security rules now past, the *Journal* will begin to cover HIPAA in other departments within "Working Smart." The editors thank Margret Amatayakul for four years of making "HIPAA on the Job" a key resource in creating privacy and security compliance programs.

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

**Article citation**:
Amatayakul, Margret. "Putting the Finishing Touches to Security--Are you Ready?" *Journal of AHIMA* 76, no.4 (April 2005): 56-57.