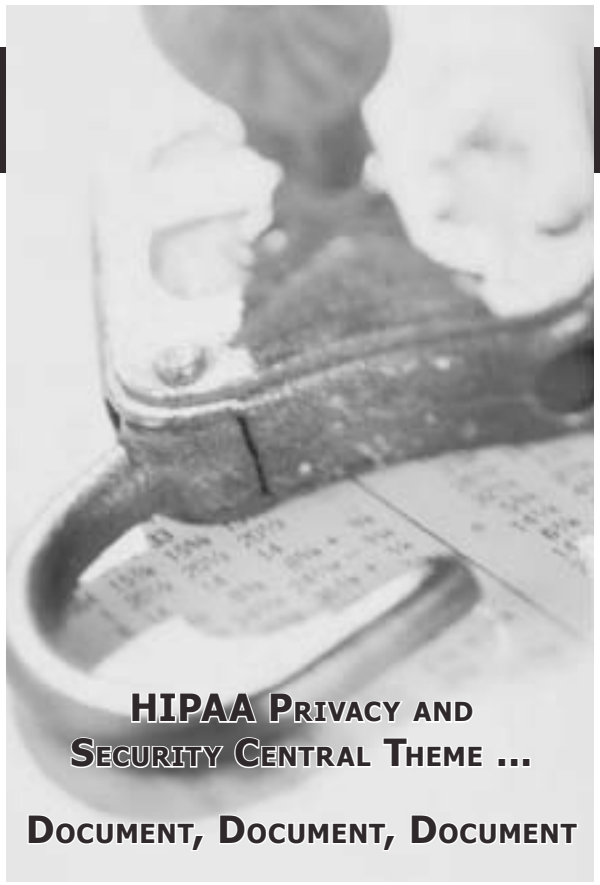
FEATURE

HIPAA Security

Roger T. Brown, CISA



You don't have to be a geek to perform a value added HIPAA Security Review. There are just over three dozen HIPAA Security control points (my term, not one used in the HIPAA Security Regulations) in the HIPAA Security Matrix (a summary table found at the end of the HIPAA Security Regulation).

Technically, the healthcare industry has been subject to HIPAA Security since the day HIPAA Privacy went live several years back. You may or may not remember Secretary Shalala considered moving back the due date of Privacy if the Security regulations weren't issued in final form in a timely manner. She obviously realized that Privacy and Security were opposite sides of the same coin.

There are two levels of audit work. At the preliminary level, which I would suggest we call a "Review" instead of an "Audit", I would find out what controls the CIO and the Security Officer think they have. It just doesn't make sense to me to test controls that the auditee knows are not in place (unless they are a very "hostile" auditee). The second level, or "Audit", tests to verify that claimed controls are actually functioning properly. Since HIPAA Security contains just over three dozen control points, make each of them an audit step and ask your CIO and Security Officer (or Privacy Officer if your organization has not yet named a Security Officer) what control process they have in place to deal with each HIPAA Security control point.

In my four years of reading practically everything I could get my hands on concerning HIPAA Privacy and Security, one central theme comes through loud and clear. Document, document, document. In this article, the most important word is not "Technology", it is "Document".

In an IT Security review I performed in 2003, I asked the Director of Network Services what control he had in place to cover "Log-in Monitoring". He replied that he received and reviewed a weekly on line report of all failed log-ons. I responded that it was a good IT control but a lousy HIPAA Security control point. What he was missing was that he had neither a procedure nor any documentation to prove he was actually performing the test. We agreed that his existing control with minor tweaking would make them "HIPAA Compliant" in this narrow area. He agreed to: (1) write a half page procedure to document the control; (2) print out the weekly report on the first Friday of every month; (3) review, sign and save the first Friday report; (4) create a log sheet of every Friday in the year; and (5) initial the date of every on line report review.

In the end, he has documented evidence that he reviewed the on line log-in failure report every week of the year. It turns out that he has a good technical control combined with adequate evidence that he has performed the control on a regular basis.

Executive management, IT, and Audit all love that kind of control: no capital expenditure, minimal IT resource usage and an effective and efficient IT control point. Oh, that we could satisfy all of the HIPAA Security control points that easily!!!

I recently attended an HFMA one-day seminar and - on a lark - selected the only HIPAA Security oriented session, "HIPAA Security for Home

Health Agencies." I am employed by a large integrated healthcare delivery system, but it was the closest topic to my areas of interest.

The speaker, who was a seasoned IT healthcare consultant, made what I considered to be a startling statement. "There is nothing in the HIPAA Security regulations that we are not already subject to." His example hit an area of personal and professional interest. Healthcare Disaster Recovery has been a major finding in almost every data center audit I have performed in the last six years. He stated that JCAHO already requires a Disaster Recovery Plan. His statement stunned me. After the session, I questioned him further and he responded that it was a JCAHO requirement, but no one on the JCAHO team was qualified to actually evaluate a Disaster Recovery Plan. One of the data center audits a peer of mine performed (and then complained incessantly to me about) had a "pretty" Disaster Recovery Plan. However, the CIO confided to her that he never expected to be able to test or invoke the plan. When I related my private discussion with the speaker from the HFMA seminar to my peer, she replied, "Now I get it." Up to that point, an "empty" (read, apparently useless) Disaster Recovery plan made no sense to a seasoned IT Auditor. But, once she realized that it was created merely to "fool" JCAHO, and maybe even Internal Audit, she clearly understood why her CIO had spent $5,000 to hire a consulting firm to develop a detailed Disaster Recovery Plan that they had no intention of being able to either test or implement.

In summary, Internal Auditors are experts in controls and documentation. If we collectively use the strengths we have and apply them to the HIPAA Security Regulations, we can both add value and significantly improve IT controls. The starting point that your organization is at today is not the most important concept. The simple fact is that HIPAA Security has higher standards than almost any of us has achieved. If you already have IT Audit on staff, you start at a high level, but unless Audit controls the organization and it has unlimited funds, IT Audit's recommendations in the past have probably been ignored, evaded or ridiculed. Now our recommendations have the force of law. If you have not had IT Audit on staff, you start at a low level of IT Security, but you now have a simple Audit Program dictated by law. Your organization has to begin to fix the IT Security weaknesses that have existed since they bought their first computer. ■

Roger T. Brown, CISA, is Senior Internal Auditor, Jefferson Health System, Radnor, PA. He spoke at AHIA's 2003 Annual Conference; he can be reached at brown@jhsmail.org.