

The undelivered promise of health privacy regulation



MY VOICE
PAUL MUGGETT

Citizens rejoice! Your medical information is now secure. All large healthcare organizations have finished implementing the final security rule of the federal HIPAA regulations as of April 2005 and your personal information is now guaranteed to be secure! Like all my best dreams, just as it is getting good my alarm clock interrupts and I awaken to the reality of a failed program. Unfortunately, not even a prescription from Dr. HIPAA can cure the problems of this federal law.

This remnant of Hillary Clinton's failed national healthcare plan is not nearly the success today's politicians claim it to be. While the HIPAA movement was well-intentioned when introduced in mid-1990, and the portability provision has been fairly successful, the reduction in healthcare costs due to standardization has not been realized. Ask anyone who has been admitted to the hospital for several days.

The security and privacy rules have been diluted to the point of uselessness while washed through the political machine and the force of special interest groups. The vagueness of the provisions presents healthcare organizations with a series of "outs" rather than providing serious requirements for securing personal information. It leaves covered entities to decide for themselves what is reasonable and appropriate for implementation and then allows them to choose an alternate method of security if the requirement doesn't match their vision. The

alternate, in some cases, is nothing more than slips of paper saying "Hey, don't do this." And why not — the government isn't checking.

In 2004, HIPAA enforcement federal dollars equaled \$10 million. That is enough money, by government standards, to perform about 10 detailed reviews of large healthcare facilities. This can hardly be interpreted as a commitment by government to ensure the protection of patients' personal information. Without a serious enforcement provision or significant funding, there isn't much incentive for healthcare organizations to take implementation seriously.

This has resulted in half-hearted compliance efforts within some healthcare ranks. From personal experience working inside the information security department of a healthcare organization, I can tell you the support for compliance simply doesn't meet the grand vision of the original HIPAA proposal. Overly-wordy security policies, poor risk assessment methods and one-time cookie-cutter awareness presentations have dominated the compliance dog-and-pony show while security best practices have been relegated to some dark backstage corner.

I doubt we can rely on government to revise its poorly developed regulation to include specific guidelines that relate to good security practices, but healthcare organizations shouldn't be let off the hook. It is reasonable to expect the healthcare industry to follow the concept of due diligence while protecting the personal information necessary to treat patients. To not do so invites disaster. Bank of America, LexisNexis, and ChoicePoint all had information security failings that compromised personal information. Is healthcare next?

At minimum, healthcare facilities, especially larger ones, should consider the following:

- Require external IT audits to support and supplement internal auditing and assessments. This provides an objective view into the security posture of the organization.

- Develop security awareness programs that are pertinent to the intended audience rather than using a one-size-fits-all approach. Knowledge is a fantastic defender of information.

- Place information security in a strategic position in the organization rather than being another IT tactical or operational function.

- Follow international best practices for security such as ISO 17799 or COBIT.

- Don't house information delivery and information security under the same reporting roof. Separation of duties, accountability, and oversight dictate untying these two distinct organizational functions.

- Create usable information security policies that are easily understood and read by the workforce. Simplicity trumps long-winded verbiage.

- Hire and retain information security experts who can relate to business objectives and provide value to the enterprise.

As patients, we expect healthcare providers to deliver exceptional treatment. Why shouldn't the same level of care be used and expected with our personal information? In this digital age, government policy has simply missed the mark. Healthcare providers cannot.

Paul Mudgett, vice president of operations with The Singleton Group in Reno, is an information security and risk management professional with over 12 years experience in regulatory compliance, technology architecture design, and incident handling. He can be reached at 996-1333.