

HIPAA – Smoke and Mirrors or Best Practice Security?

The final Security Standards for the Health Insurance Portability and Accountability Act of 1996 (HIPAA) hit the street on April 21, 2003. The first compliance date for most entities looms just around the corner - April 21, 2005. Still, many affected firms have not started on the security portion of this Act.

Why not? With many references like § 164.308(a)(4)(ii)(B), Subpart this, and sub-title that, the Standards seem intimidating, complex and mystic. At first look, one might think it is easy to misinterpret the requirements. But with a closer look, one finds there is no “smoke and mirrors” magic behind the final HIPAA regulations. After all of the comments and responses to those comments, the resulting final HIPAA Security Standard is a very straightforward, comprehensive, best practice security guide, complete with references, a requirements matrix in Addendum A for guidance, and a reference guide in Addendum C for security best practice help.

An explanation of where the Security Standards originate might help eliminate some of the confusion. In actuality, these are not healthcare-specific recommendations, but rather general steps every business, university and even home Internet user should consider. The standard contains many references to NIST (the National Institute of Standards and Technology). NIST is a non-regulatory federal agency within the U.S. Commerce Department charged with developing and promoting measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life. This mission touches everything from volume (the amount of milk in a gallon), to time (the “official” US clock), to the best ways to secure a network. Most of NIST Information Technology Security Standards can be found in the “800” series, including all NIST references made in the final HIPAA publication.



For example, Addendum 3 of the Act is a cross-reference of sections to readily available publications. “47” is from NIST – Generally Accepted Principles and Practices for Secure Information Technology Systems. The cross reference is NIST SP 800-14.

The Federal Register publication further says that industry best practice security such as NIST can be followed, but other standards could be used as well. The SANS Institute (<http://www.sans.org>), noted as one of the best resources for security collaboration, is currently in process of finalizing their guide to HIPAA compliance.

While not mysterious or obscure, one could accurately describe HIPAA security as multifaceted. The solutions to each facet may not be complex, but the entire process of best practice security does cover a wide array of issues in an environment. This challenge does not lend itself to a “silver bullet” approach. Some advertisements seem to indicate that a certain product is a “Solution for HIPAA Compliance”. While straightforward and technology-neutral, HIPAA security requirements do cover a wide range of technologies and elements. It is a stretch to think that one product could cover everything from physical security, to policies, to procedures, to incident handling.

However, that is not to say that one company qualified in implementing Risk Management and Information Security practices may not be able to guide a healthcare entity to compliance.

The final publication is a “what to do” guide, not a “how to do it” document. This presents a good foundation for the vast diversity in size of organizations, variances in business models, and breadth of technology requirements from network to network. The Security Standards provide for technology neutral solutions. This allows for flexibility and scalability for each environment, as well as technologic advances and ever evolving environments and requirements. In other words, USE BEST PRACTICE SECURITY TO MEET THE REQUIREMENTS. This theme is re-enforced over and over throughout the final HIPAA security standards.

The Standards also list elements as “addressable” (A) or “required” (R). The (A) indicator does not imply that the entity can decide to not implement a solution for that issue. Rather, it gives the entity the latitude to address the issue in an appropriate manner. A risk assessment may determine that the item is not a risk, and thus proper documentation concerning that conclusion is appropriate.

Thirteen elements were listed as “required” (R) and are to be implemented. Risk Analyses is a large part of Risk Management and both are required elements for compliance. This is a logical first step for any organization to implement best security practices. Properly undertaken, a risk assessment will provide a complete list of the hardware, policies, procedures, physical security and training needed for HIPAA compliance.

So, no smoke and mirrors, no silver bullets, just roll up your sleeves and dig in. Run a risk analysis on every system, find the risks and the associated impacts, write your mitigation strategies, get your risk management program in action, implement your plans, and follow the guidelines and good old industry best practice security to take you down the road to HIPAA compliance.

Rebecca Cosby, CISSP
Senior Security Consultant
TechGuard Security

TechGuard Security®
743 Spirit 40 Park Drive, Suite 206
Chesterfield, MO 63005
Phone: 636.519.4848
Fax: 636.519.4850
Email: info@techguardsecurity.com
www.techguardsecurity.com