

AAHP-HIAA

**NATIONAL COMMITTEE ON VITAL HEALTH STATISTICS
SUBCOMMITTEE ON STANDARDS AND SECURITY**

IMPLEMENTATION OF THE HIPAA SECURITY RULE

**PRESENTATION BY TOM WILDER
VICE PRESIDENT, PRIVATE MARKET REGULATION**

AAHP-HIAA

January 27, 2004

Tom Wilder
Vice President, Private Market Regulation
AAHP-HIAA
601 Pennsylvania Avenue
Suite 500, South Building
Washington, D.C. 20004
(202)778-3255
twilder@aahp.org

Good afternoon. My name is Tom Wilder and I am Vice President of Private Market Regulation for AAHP-HIAA. AAHP-HIAA is the national trade association representing the private sector in health care. AAHP-HIAA's nearly 1,300 member companies provide health, long-term care, dental, vision, disability, and supplemental coverage to more than 200 million Americans. I would like to thank you for the opportunity to testify today on the challenges that health plans face in implementing the HIPAA Security Rule.

Technological advances allow new, innovative ways to create, transmit, and store health information. Such advances are also accompanied by a new potential for unauthorized access to health information -- modern-day computer hackers, weak internet and other communication system portals, and lax information handling and disposal practices can allow these potential threats to become a reality. The HIPAA Security Rule that was finalized on February 20, 2003 is intended to assist covered entities by establishing requirements for policies and procedures and operational steps to protect health information from unauthorized access or modification.

Implementation of the Security Rule

As you are aware, most covered entities have until April 20, 2005 to come into compliance with the Security Rule (small health plans have until April 20, 2006 to comply). Health plans and insurers are making significant progress toward implementation of the rule and are instituting the necessary physical and electronic data transmission security safeguards, training workforce members, and developing required

policies and procedures. In many cases, health plans and insurers have already instituted additional security protections as part of the implementation process for the HIPAA Privacy Rule, which requires covered entities to protect against the unauthorized use and disclosure of health information.

Health plans and insurers have reported a number of challenges in implementation of the HIPAA Security Rule, including the following:

- Adapting “off the shelf” security products and security functions of software products such as Microsoft XPTM.
- Establishing security protocols for workforce members who work from home (or other locations out of the office) and for business associates (such as consultants) that handle data off-site.
- Developing logging and monitoring procedures for data use.
- Setting up procedures and systems to authorize access to data that distinguish between levels of access based on the individual’s position or job description (i.e., “role-based” access).
- Monitoring activities of business associates.

Health plans and insurers have focused their efforts on addressing these key issues as they work to come into compliance with the rule.

“Scalable” Requirements for Health Information Security

The preamble to the Security Rule makes clear that the rule’s provisions are intended to be scalable and flexible requirements based upon the unique needs and business

operations of each covered entity. Many of the requirements are “addressable,” meaning that a covered entity can determine whether implementing a particular specification is a reasonable and appropriate safeguard for the covered entity’s operations. This approach allows health plans and insurers to assess their own particular needs when deciding how best to implement the Security Rule. **AAHP-HIAA supports a scalable and flexible implementation process for the Security Rule based on each covered entity’s business needs and operations.**

Security Rule Enforcement

The Centers for Medicaid and Medicare Services (CMS), has responsibility for enforcement of the HIPAA Administrative Simplification requirements related to electronic health care transactions, including the Security Rule. The rule sets out new expectations and business requirements for many covered entities and it is important that CMS work with covered entities on implementation rather than taking a strictly proscriptive approach to its enforcement activities. **AAHP-HIAA supports the approach taken by CMS to enforce the HIPAA Security Rule through assisting covered entities with their development of security safeguards.**

Need For Additional CMS Education and Outreach

Providing covered entities the flexibility to adapt the HIPAA Security Rule to their own unique business and operational needs is appropriate, however, it would be helpful if CMS could provide additional education and outreach to assist covered entities in their efforts to implement the rule. While CMS has understandably been busy with its efforts

to assist covered entities with implementation of the HIPAA electronic transactions rule, the agency should increase its efforts to provide outreach and educational activities related to the Security Rule. For example, CMS could develop educational seminars and roundtable discussions and resource materials geared toward specific audiences, such as health care providers and employers, to help them understand the implications of the Security Rule and how they can best come into compliance. **AAHP-HIAA recommends that CMS provide targeted education and outreach to covered entities through brochures, seminars, “checklists” and other materials on compliance with the Security Rule. AAHP-HIAA is ready to partner with CMS in these efforts.**

Conclusion

AAHP-HIAA and its member companies have long supported protections for the privacy of health information. The HIPAA Security Rule advances this goal by setting uniform industry standards for basic safeguards of electronically maintained or transmitted health information. AAHP-HIAA is committed to work with its members to implement the HIPAA Security Rule.