

Implications of HIPAA on the Telecommunications Market

What we refer to as HIPAA is technically Public Law 104-191, the Health Insurance Portability and Accountability Act of 1996. It was designed "to amend the Internal Revenue Code of 1986 to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes."

While the implications and requirements for HIPAA are quite broad and include support for electronic exchange of information, many health care organizations have already worked diligently to implement some form of EDI. In this paper, we're going to consider some of the security issues that impact the industry.

Legal Implications for the Healthcare Industry

From the perspective of the IT department, this means that the health care industry now has to get on the information and content security bandwagon and start protecting patient information, and be held accountable for it.

Many will argue that in the past the health care industry chose profit over security and the patient's right to privacy. Even the Hippocratic oath mentions confidentiality of patient information by stating "Whatever, in connection with my professional practice or not in connection with it, I see or hear, in the life of men, which ought not to be spoken of abroad, I will not divulge, as reckoning that all such should be kept secret." Now the entire healthcare industry finds itself under stringent requirements to comply with the law, and is scrambling to institute security policies and procedures to avoid government imposed penalties for non-compliance with the Act. It's imperative to note that wrongful disclosure of information is classified as a felony offense.

From a security viewpoint, this means some safeguards must be implemented:

- Ensure the integrity and confidentiality of information
- Protect against any reasonably anticipated threats or hazards to the security or integrity of the information; and unauthorized uses or disclosures of the information.
- Use electronic signatures for non-repudiation.

While the impact of HIPAA is new to the health care industry, the requirements are very similar to site based certification and accreditation of computer systems within the Federal Government, particularly agencies like the Department of Defense. Some excellent resources to understand and prepare for HIPAA are some of the preceding acts:

- The Privacy Act of 1974, PL 93-579
- Computer Security Act of 1987, PL 100-235
- National Security Decision Directive Number 145, National Policy on Telecommunications and Automated Information Systems Security

Implications for Network Service Providers

As is always the case when a new law is enacted, somebody is going to make a lot of money. Just make sure it's you and your organization, and not the competition.

For many of us in the telecommunications industry, this means our clients are either expanding or creating the role of the Information Security Manager. The Department of Health and Human Services Security and Electronic Signature Standards requires that "security responsibility be designated to a specific individual or organization and the assignment be documented. These responsibilities include the management and supervision of security measures to protect data, and conducting training of personnel in relation to the protection of data. This assignment is important in providing an organization focus and importance to the security and pinpointing of responsibility."

This new role has some requirements that include:

- Monitoring compliance with the organizations information security policies and procedures for all employees, contractors, alliances and other third parties.
- Monitoring internal control systems to ensure that appropriate information access levels and security clearances are maintained.
- Performing information security risk analysis.
- Serve as an internal security consultant to the organization.
- Monitor changes in legislation and accreditation standards that affect information security.
- Initiate, facilitate and promote activities to foster information security awareness within the organization.

Development of a security program and setting security policies requires the active involvement of all stakeholders within an organization, and is best approached by forming a cross-functional team encompassing all areas of both the business and patient care departments. This cross-functional team is where the telecommunications service provider can bring a solid understanding of systems and network security to the table, but in many cases, it will be that service provider who helps and organization establish the cross-functional team to begin.

In order to help our customer understand the growing requirements on their own networks and data centers, we must also research and understand the requirements enacted by HIPAA. In the telecommunications sector, a first resource will be those departments that already work supporting Federal Government agencies like the Department of Defense. These groups already have a foundation of working with and understanding certification and accreditation requirements similar to those required under the Act.

Several organizations publish regular updates on information security standards:

- American Health Information Management Association (AHIMA), www.ahima.org
- National Institute of Standards and Technology, Computer Security Division, www.itl.nist.org
- Computer-based Patient Record Institute (CPRI), www.cpri.org
- Information Systems Security Association (ISSA), www.issa.org

- International Computer Security Association (ICSA), www.icsa.net

Most studies indicate that the time and money invested in HIPAA compliance overall have been relatively modest so far. For much of the health care industry, the work and stress of the Y2K projects they dealt with left them unprepared to tackle another large initiative so quickly. This means that the clock is ticking, and these groups are going to need help from their service providers.

The healthcare industry needs assistance in wading through the quagmire of VPN options available today. While ATM and Frame Relay provide VPN-like privacy, they don't inherently offer any form of encryption. MPLS based VPNs again provide privacy, but encryption make be critical to ensuring the privacy of patient records.

The requirement for implementation of digital signatures coupled with privacy requirements certainly points to many of the IPsec Virtual Private Network (VPN) offerings that provide cryptographic solutions for privacy and the use of X.509 digital certificates to implement the digital signature. Even though the VPN marketplace is still achieving critical mass, the IPsec VPN has become the gold standard for sending private information over the Internet, which will play a crucial role in individuals' access to their own records and information.

In addition to VPN technology, many healthcare organizations will now be looking to using Secure Sockets Layer (SSL) or Transport Layer Security (TLS) as a means of providing web-based access to information by individuals via the Internet. This is going to necessitate secure web servers, comprehensive firewalls, and intrusion detection systems far and wide throughout the healthcare sector.

Security has always been a critical, but often under appreciated facet of the telecommunications network, particularly the Internet. For the health care industry, this has changed dramatically as a direct result of the Act.

As service providers we often advertise the value we bring to our customers. Certainly within the service provider industry, we have wide ranging knowledge of network security options and solutions. This is the time for us to take that value, that fundamental knowledge, to the health care industry and deliver the information and wisdom they need to make informed, intelligent decisions.

We must help them evaluate their requirements and take action now while there is time to comply with the regulations. Those organizations that delay will only find themselves faced with deadlines that can't be extended, and intervals that become impossible to meet as the required dates draw near.

Ken Camp, Member of Technical Staff
Hill Associates, Inc. www.hill.com
106 Highpoint Center
Colchester, VT 05446
(802) 655-0940
k.camp@hill.com