Sanctum Security Advisory

SANCTUM

Government Regulations

Health Insurance Portability and Accountability Act (HIPAA)

The Administrative Simplification section of HIPAA mandates a new security policy to protect an individual's health information, while permitting the appropriate access and use of that information by health care providers, clearinghouses and health plans. As part of a broad Congressional attempt at incremental healthcare reform, HIPAA sets mandates for security standards and guidelines to standardize and increase electronic data exchange (EDI) in order to facilitate a more efficient exchange of information throughout the healthcare system.

HIPAA covers all medical records and other *individually identifiable health information* used or disclosed in any form by hospitals, health plans, health care clearinghouses, and health care providers, from large integrated delivery networks to individual physician offices. This represents over 4M health plans and 1.2M providers. While the easy transfer of medical records has the potential to streamline healthcare processes and greatly reduce costs, it dramatically increases the risk of inappropriate access to sensitive information. Therefore, HIPAA sets distinct regulations for both the privacy requirements for information to be kept confidential, and the **security standards** to ensure that it does.

Rulings for Privacy and Security include:

- **Privacy Ruling** - *Disclosing Data* (compliance by 4/14/2003) the need for information security to ensure privacy is delineated: "It is the responsibility of organizations that are en trusted with health information to protect it against deliberate or inadvertent misuse or disclosure".
- **Security Ruling** – *Protecting Data* (Proposed: 8/12/1998)[1] mandates safeguards for physical storage and maintenance, transmission and access to individual information.

Mandates for Security Standards:

Ensure the integrity and confidentiality of electronic health 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.

Provide technical security services to guard data integrity, confidentiality, and availability.

- — Audit controls – Each organization is required to have audit control mechanisms to record and examine system activity. Therefore, an organization can identify suspect data access, assess its security program and respond to potential weak nesses.

Penalties for non-compliance to HIPAA:

- *Wrongful Disclosure of Individually Identifiable Health Information:* $50,000 and/or not more than one-year imprisonment
  (1) Uses or causes to be used a unique health identifier;
  (2) Obtains individually identifiable health information relating to an individual; or,
  (3) Discloses individually identifiable health information to another person.
- Lawyers warn of the possibility of private suits under existing state tort laws. HIPAA's general privacy and security requirements have been enforceable law since 1996. Lawyers argue that a high level of care needs to be realized where security of individually identifiable health information is at stake in order to prevent a private plaintiff negligence suit.

Summary of HIPAA:

HIPAA requires the development of comprehensive security programs to protect healthcare data. Analysts are concerned that healthcare organizations have been slow to adopt the regulations and patient information remains unprotected. Larger than the penalties for non-compliance is the threat of private plaintiff suits and that patients will take their business elsewhere. Gartner Group says that unless substantial progress is made in the next three months, the healthcare industry won't be ready to meet the first **April 14, 2003** deadline.

[1] Standards are required to be implemented within 2 years of the effective date of the final rule; (The effective date of the final rule is generally 60 days after its publication.) The final rule has not yet been published.

▪ By October 16, 2003, providers must submit all claims electronically to Medicare.

SANCTUM

How Sanctum Aids Compliance to the HIPAA:

Based on statistics, a clear anticipated threat is that hackers will try and exploit security holes to access healthcare data enabling organizations to *wrongfully disclose individually identifiable health information.*

- Hackers victimized 90% of large corporation and government agencies within the last 12 months (Computer Security Institute and FBI).
- 75% of the malicious attacks on the Web occur at the application level (Gartner Group).

A security policy, therefore, must specifically address the threat to the application level, where data is most vulnerable, in order to comply with HIPAA.

AppShield and AppScan are the only solutions in the market today that can ensure accelerated compliance to HIPAA privacy and security standards.

APPSHIELD BENEFITS

- Provides 24/7 automatic defense against reasonably anticipated *"threats or hazards to the security or integrity of the information"* as well as unknown threats or security vulnerabilities, as **required by the law**.
- Blocks all suspicious activity launched against a web application by creating dynamic security policies, thus ensuring the integrity and confidentiality of the information.
- Provides the audit control mechanisms to record and examine system activity as **required by the law.**
- Logs all requests that reach the Web server and acts as a forensics tool to identify suspect data access activities and help catch hackers, as **required by the law**.
- Keeps pace with technology, **required by the law**, by intelligently and automatically defining policy on the fly for any custom or 3rd party application.

APPSCAN BENEFITS

- Automated vulnerability assessment tool to help QA, auditors and developers secure the code of healthcare Web sites and identify the potential areas where site security could be compromised.
- Provides automated *"audit control mechanisms to record and examine system activity"*, as **required by the law**, and enables healthcare organizations to be proactive in fixing application vulnerabilities that might *disclose individually identifiable health information.*
- Improves the efficiency of Web application audits by up to 500%.
- Examines the output of the application source code and supports third party and custom-built applications, eliminating potential vulnerabilities found in code generated by companies that are not held to the same stringent data protection laws as healthcare organizations.