HIPAA Compliance and FMAudit Products

Introduction

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) established a mechanism for the establishment of rules and regulations to protect the privacy of patient's health information.

In November 1999, HHS published proposed regulations to guarantee patients new rights and protections against the misuse or disclosure of their health records. In December 2000, HHS issued a final rule, and after a comment period, President Bush and Health and Human Services Secretary Thompson decided to allow the rule to take effect on April 14, 2001. As required by the HIPAA law, most covered entities have two full years - until April 14, 2003 - to comply with the final rule's provisions. The law gives HHS the authority to make appropriate changes to the rule prior to the compliance date.

Covered Entities: As required by HIPAA, the final regulation covers health plans, health care clearinghouses, and those health care providers who conduct certain financial and administrative transactions (e.g., electronic billing and funds transfers) electronically.

Information Protected: All medical records and other individually identifiable health information used or disclosed by a covered entity in any form, whether electronically, on paper, or orally, are covered by the final rule.

Network Security and Certification

The HIPAA regulations do not provide for a central testing or authentication of any procedure, device, or system. This was a component of the design of the HIPAA regulations, as published by HHS:

"The final rule establishes the privacy safeguard standards that covered entities must meet, but it gives covered entities the flexibility to design their own policies and procedures to meet those standards. The requirements are flexible and scalable to account for the nature of each entity's business, and its size and resources."

FMAudit products are currently installed at a number of sites which must comply with the HIPAA regulations for security and confidentiality. Based on the current regulations, no "authority" is given to anyone to "certify" a solution that is the responsibility for the security officer for the client company. This document shows how FMAudit products are designed to be compliant with the strictest interpretations of the regulations.

Very specific guidelines are provided to each regulated entity to assist in their own investigation and certification of components of their system. Included at the end of this document are the official security checklists as published by HHS, excerpts from networking vendor Cisco's published white paper, excerpts from *For The Record:*

Protecting Electronic Health Information (the report of the Committee on Maintaining Privacy and Security in Health Care Applications, upon which much of the regulations are based), and a more complete excerpt of the HHS fact sheet on HIPAA compliance.

FMAudit products Architecture and the HIPAA regulations

The FMAudit products are fully compliant with the HIPAA regulations because:
The FMAudit products do not store, process, monitor or manage any patient records or any records or information that is specific to any one patient or group of patients. The product engines communications are controlled, using limited access to contact a specific IP address and/or ranges. All communications must originate from the FMAudit products (outbound communication through the firewall), and there is no way to contact and access the products from outside the network. The communication outside of the network uses a proprietary, compressed data stream wrapped with 256 bit encryption with password protection.

The FMAudit products report the usage counts (meter readings) status of print devices on the network. It does not communicate any information about any specific print jobs. While the devices might print out patient records, FMAudit products do not and can not determine anything about the information being printed. It only performs audits, on a scheduled basis, the meter readings of the device, or in the case of a device problem, an alert (i.e. out of toner or door open).

The FMAudit products cannot in any way be configured to perform a task beyond the ones for which it was designed. The transmission of data from the products to outside sources is tightly restricted. The products do not report any other details except for information of the equipment being monitored (i.e. type of equipment or its IP address). No patient related information ever leaves the network via FMAudit products.

Summary

While every network security administrator must make their own decisions on HIPAA compliance of all systems and devices, as is required by regulation, the FMAudit products can be completely investigated and when HIPAA compliance regulations are compared to the products and security, there will be no areas of compromised security of patient records with the products installed on the network monitoring printers and other print output devices. The device does not deal with patient records in any way, and the network monitoring of print devices that it does will not compromise any of the protected data. The device is a single purpose device and cannot be reprogrammed by someone else to perform any other tasks.

IHS HIPAA Security Checklist

a. **Administrative procedures to guard data integrity, confidentiality, and availability**

   1) **Certification** - 142.308(a)

      ❖ **Risk Analysis**—Complete Facilitated Risk Assessment (FRA) and analyze results

      ❖ **Risk Management**—Implement security plans resulting from FRA

      ❖ **Security Policy**—Review and update as necessary

   2) **A Chain of Trust Partner Agreement** - 142.308(a)

      ❖ Establish chain of trust partner agreements with all business partners with which IHS exchanges PHI

   3) **A Contingency Plan -** 142.308(a)

      ❖ **Applications and Data Criticality Analysis**—Complete development

      ❖ **Data Backup Plan**—Complete review

      ❖ **Disaster Recovery Plan**—Complete review

      ❖ **Emergency Mode Operation Plan**—Complete review

      ❖ **Testing and Revision Process**—Complete review

   4) **Formal Mechanism for Processing Records** - 142.308(a)

      ❖ Review and update content as appropriate

   5) **Information Access Control** - 142.308(a)

      ❖ **Access Authorization**—Review and update access authorization

      ❖ **Access Establishment**—Review and update access definitions

      ❖ **Access Modification**—Review and update rules for modifying access

   6) **Internal Audit** - 142.308(a)

      ❖ Review and update content as appropriate

   7) **Personnel Security** - 142.308(a)

      ❖ **Assuring supervision of maintenance personnel by an authorized, knowledgeable person**—Complete procedure

      ❖ **Maintaining a record of access authorizations**—Complete procedure

- ❖ **Assuring that operating and maintenance personnel have proper access authorization**—Develop or update procedure as necessary
- ❖ **Establishing personnel clearance procedures**—Update procedure as necessary
- ❖ **Establishing and maintaining personnel security policies and procedures**—Update procedure as necessary
- ❖ **Assuring that system users, including maintenance personnel, receive security awareness training**—Update procedure as necessary

8) **Security Configuration Management** - 142.308(a)
   - ❖ **Documentation**—Complete security plans, rules, and procedures
   - ❖ **Hardware and software installation and maintenance review and testing**
   - ❖ **for security features**—Update procedures as necessary
   - ❖ **Inventory**—Update inventory as necessary
   - ❖ **Security testing**—Complete procedures
   - ❖ **Virus checking**—Compliant

9) **Security Incident Procedures** - 142.308(a)
   - ❖ **Report Procedures**—Complete procedures
   - ❖ **Response Procedures**—Complete procedures

10) **Security Management Process** - 142.308(a)
   - ❖ **Risk Analysis**—Will be repeated every three years or upon significant system changes
   - ❖ **Risk Management**—Implement continuous process
   - ❖ **Sanction policies and procedures**—Make a part of the annual security training
   - ❖ **Security policy**—Make a part of the annual security training

11) **Termination Procedures** - 142.308(a)
   - ❖ **Changing locks**—Review compliance as a part of the recurring Risk Analysis
   - ❖ **Removal from access lists**—Review compliance as a part of the recurring Risk Analysis

- ❖ **Removal of user account(s)**—Review compliance as a part of the recurring Risk Analysis

- ❖ **Turning in of keys, tokens, or cards that allow access**—Review compliance as a part of the recurring Risk Analysis

12) **Training** - 142.308(a)

- ❖ **Awareness training for all personnel, including management personnel**—Review compliance as a part of the recurring Risk Analysis

- ❖ **Periodic security reminders**—Review compliance as a part of the recurring Risk Analysis

- ❖ **User education concerning virus protection**—Review compliance as a part of the recurring Risk Analysis

- ❖ **User education in importance of monitoring log-in success or failure and how to report discrepancies**—Review compliance as a part of the recurring Risk Analysis

- ❖ **User education in password management**—Review compliance as a part of the recurring Risk Analysis

b. **Physical safeguards to guard data integrity, confidentiality, and availability**

1) **Assigned Security Responsibility -** 142.308(b)

- ❖ No action required

2) **Media Controls -** 142.308(b)

- ❖ Implement changes as necessary

3) **Physical Access Controls -** 142.308(b)

- ❖ **Disaster Recovery**—Update procedures as necessary
- ❖ **An Emergency Mode Operation**—Update procedures as necessary
- ❖ **Equipment Control**—Update controls as necessary
- ❖ **A Facility Security Plan**—Update procedures as necessary
- ❖ **Procedures For Verifying Access Authorizations Before Granting**
- ❖ **Physical Access**—Update procedures as necessary
- ❖ **Maintenance Records**—Update record content as necessary

❖ **Need-To-Know Procedures For Personnel Access**—Update procedures as necessary

❖ **Procedures To Sign In Visitors And Provide Escorts, If Appropriate**—Update procedures as necessary

❖ **Testing And Revision**—Update procedures as necessary

4) **Policy and Guidelines On Work Station Use -** 142.308(b)

❖ Update existing policy and guidelines as necessary

5) **A Secure Work Station Location -** 142.308(b)

❖ Update policy as necessary

6) **Security Awareness Training -** 142.308(b)

❖ Update existing policy as necessary

c. **Technical security services to guard data integrity, confidentiality, and availability**

1) **Access Control** - 142.308(c)(1)(i)

❖ **Procedure for Emergency Access**—Update the existing policy as necessary

❖ **Context-, Role-, or User-based Access**—Update the existing policy as necessary

2) **Audit Controls** - 142.308(c)(1)(ii)

❖ Update audit controls as necessary and implement consistently

3) **Authorization Control** - 142.308(c)(1)(iii)

❖ Update authorization controls as necessary

4) **Data Authentication** - 142.308(c)(1)(iv)

❖ Develop and implement authentication controls as necessary

5) **Entity Authentication** - 142.308(c)(1)(v)

❖ Implement dual factor authentication when feasible

d. **Technical Security Mechanisms**

1) **Communications or Network Controls** - 142.308(d)

Both of the following:

❖ **Integrity Controls**—Implement new integrity controls as necessary

❖ **Message Authentication**—Implement new authentication controls as necessary

One of the following:

❖ **Access Controls**—No action necessary

❖ **Encryption**—Implement for open network transmission

2) **Implementation Features** - 142.308(d)

❖ **Alarm**—Implement new features as necessary

❖ **Audit Trail**—Implement new audit controls as necessary

❖ **Entity Authentication**—Implement two factor authentication as feasible

❖ **Event Reporting**—Implement new tools as necessary

Excerpt from Cisco Systems published white paper on network security and HIPAA:

HIPAA recommends several requirements that should be included in the final health care security standard to protect the integrity, confidentiality, and availability of electronic health data. For the purposes of presentation only, the proposed requirements were divided within HIPAA into the following four categories:

- **Administrative procedures**—Documented formal practices to manage the selection and execution of security measures to protect data and the conduct of personnel in relation to the protection of data. Administrative procedures would include such items as formal termination procedures, security incident procedures, and security training.

- **Physical safeguards**—Relate to the protection of physical computer systems, buildings, and equipment from fire, environmental hazards, and physical intrusion. Physical safeguards also cover the use of locks, keys, and administrative measures that control access to computer systems and facilities.

- **Technical security services**—Include the processes to protect, control, and monitor information access, such as access control and data authentication.

- **Technical security mechanisms**—Include the processes to prevent unauthorized access to data transmitted over a communications network, such as encryption, event reporting, integrity controls, and audit trails.

HIPAA Takes a General Approach

HIPAA recommends general requirements for the prospective security standard, rather than mandating specific security technologies for implementation in health care networks. HIPAA also suggests that organizations assess the potential security risks to the health information in their possession and determine which specific technologies will best meet their particular security and overall business needs. This approach was supported by one of many research reports consulted by the creators of HIPAA. The National Research Council's 1997 report, *For The Record: Protecting Electronic Health Information,* states, "It is therefore not possible to prescribe in detail specific practices for all organizations; rather, each organization must analyze its systems, vulnerabilities, risks, and resources to determine optimal security measures. Nevertheless, the committee believes that a set of practices can be articulated in a sufficiently general way that they can be adopted by all health care organizations in one form or another."

Cisco Systems White Paper

Security and Authentication from
For The Record: Protecting Electronic Health Information

Authentication is any process of verifying the identity of an entity that is the source of a request or response for information in a computing environment. It is the linchpin for making decisions about appropriate access to health care information, just as it is for controlling legal and financial transactions. Generally, authentication is based on one or more of four criteria:

- Something that you have (e.g., a lock key, a card, or a token of some sort);

- Something that you know (e.g., your mother's maiden name, a password, or a personal ID number);

- Something related to who you are (e.g., your signature, your fingerprint, your retinal or iris pattern, your voiceprint, or your DNA sequence); or

- Something indicating where you are located (e.g., a terminal connected by hardwired line, a phone number used in a callback scheme, or a network address).

Access Control Technologies Observed on Site Visits

The committee's review indicated that most health care organizations are attempting to adapt access control criteria and processes from paper record systems to on-line systems. Thus, most sites conceptually identify four classes of information:

- Public information (e.g., promotional materials, educational materials) available to any interested person inside or outside the organization;

- Internal confidential information (e.g., organizational policies, business strategies, outcomes and utilization information) accessible on a need-to know basis to organization employees and affiliates;

- Confidential patient record information - the routine content of patient health records - accessible on a need-to-know basis to providers and oversight groups, as well as to outside groups (e.g., insurance payers); and

- Highly sensitive patient record information (e.g., records of celebrities or other widely recognized persons, or special content such as information related to substance abuse, psychiatric care, physical abuse, HIV status, and abortions) accessible on a restricted need-to-know basis to authorized users of patient record information.

For The Record: Protecting Electronic Health Information

Committee on Maintaining Privacy and Security in Health Care Applications of the
National Information Infrastructure; Computer Science and Telecommunications
Board ;Commission on Physical Sciences, Mathematics, and Applications; and National
Research Council

US Department of Health and Human Services (HHS)
HIPAA Fact Sheet Excepts

PROTECTING THE PRIVACY OF PATIENTS' HEALTH INFORMATION

__Overview:__ Each time a patient sees a doctor, is admitted to a hospital, goes to a pharmacist or sends a claim to a health plan, a record is made of their confidential health information. In the past, family doctors and other health care providers protected the confidentiality of those records by sealing them away in file cabinets and refusing to reveal them to anyone else. Today, the use and disclosure of this information is protected by a patchwork of state laws, leaving gaps in the protection of patients' privacy and confidentiality.

Congress recognized the need for national patient record privacy standards in 1996 when they enacted the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The law included provisions designed to save money for health care businesses by encouraging electronic transactions, but it also required new safeguards to protect the security and confidentiality of that information. The law gave Congress until August 21, 1999, to pass comprehensive health privacy legislation. When Congress did not enact such legislation after three years, the law required the Department of Health and Human Services (HHS) to craft such protections by regulation.

In November 1999, HHS published proposed regulations to guarantee patients new rights and protections against the misuse or disclosure of their health records. During an extended comment period, HHS received more than 52,000 communications from the public. In December 2000, HHS issued a final rule that made significant changes in order to address issues raised by the comments. To ensure that the provisions of the final rule would protect patients' privacy without creating unanticipated consequences that might harm patients' access to care or quality of care, HHS Secretary Tommy G. Thompson opened the final rule for comment for 30 days. After that comment period, President Bush and Secretary Thompson decided to allow the rule to take effect on April 14, 2001, as scheduled, and make appropriate changes in the next year to clarify the requirements and correct potential problems that could threaten access to or quality of care. Secretary Thompson's statement on this issue is available at http://www.hhs.gov/news/press/2001pres/20010412.html.

BOUNDARIES ON MEDICAL RECORD USE AND RELEASE
With few exceptions, such as appropriate law enforcement needs, an individual's health information may only be used for health purposes.

- **Ensuring that health information is not used for non-health purposes.** Health information covered by the rule generally may not be used for purposes not related to health care - such as disclosures to employers to make personnel decisions, or to financial institutions - without explicit authorization from the individual.

- **Providing the minimum amount of information necessary.** In general, disclosures of information will be limited to the minimum necessary for the purpose of the disclosure. However, this provision does not apply to the disclosure of medical records for treatment purposes because physicians, specialists, and other providers need access to the full record to provide quality care.

ENSURE THE SECURITY OF PERSONAL HEALTH INFORMATION

The final rule establishes the privacy safeguard standards that covered entities must meet, but it gives covered entities the flexibility to design their own policies and procedures to meet those standards. The requirements are flexible and scalable to account for the nature of each entity's business, and its size and resources. Covered entities generally will have to:

- **Adopt written privacy procedures.** These include who has access to protected information, how it will be used within the entity, and when the information may be disclosed. Covered entities will also need to take steps to ensure that their business associates protect the privacy of health information.

- **Train employees and designate a privacy officer.** Covered entities will need to train their employees in their privacy procedures, and must designate an individual to be responsible for ensuring the procedures are followed.

US Department of Health and Human Services