GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

HIPAA Compliance: Role Based Access Control Model
Kenneth Cole, v1.2f

The time is running out on the biggest information management project the healthcare industry has ever faced. In August of 2000, the Department of Health and Human Services (HHS) published the first set of rules – Standards for Electronic Transactions and Code Sets – under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), also known as Public Law 104-191. In December, the HHS published the next set – Standards for Privacy of Individual Identifiable Health Information. There are more final rules coming and some are expected before the end of 2001.

The HHS Fact Sheet titled "Protecting the Privacy of Patients' Health Information" summarizes the situation:

> Congress recognized the need to 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 save guards 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. (HHS, Overview)

Most healthcare entities will have 24 months from the effective date of each rule to achieve compliance. Two years may seem like enough time to meet the requirements of these regulations, but experts recommend that organizations begin as soon as possible. Waiting until the last few months to initiate strategic measures will cause undue stress and could mean failure to meet the deadlines.

Only two of these standards have been published in final form, but the remaining documents are expected to be published soon. The four areas are:

- **Transactions and Code Sets Standards** for formal standardization of electronic communication of health, administrative, and financial data relating to patients. Compliance is required on October 16, 2002 – 60-days plus 24-months after the publication of the final rule;

- **Privacy and Confidentiality Standards** for guaranteeing the patient's right of confidentiality of their personal health information. Compliance is required on April 14, 2003;

- **Security and Electronic Signature Standards** for protection of the confidentiality, integrity, and availability of individual health information; and

- **Unique Identifiers** for individuals, employers, health plans, and health care providers.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Although it has not been published in final form, the Security and Electronic Signature Standards may present the most challenges for healthcare organizations and their information management teams. A primary component of the security standard is the implementation of access controls to protect the confidentiality of individual health information. The purpose of this paper is to offer an approach to managing user access to information that will meet the HIPAA security requirements for individual health data management.

HIPAA Security Standards

The HIPAA security standards have been created to ensure confidentiality and integrity of individual health information. There is no current consistent protection of individual health information. HIPAA's security standards would establish a minimum standard for the protection of individual health information that is stored electronically or transported over telecommunication systems. The standards also provide for controlled access to appropriate covered entities.

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

The security standards are to apply to all individual health information that is in electronic form, whether stored or in transit. That is, they apply not only to administrative and financial healthcare transactions covered by the HIPAA transaction standards, but also to any and all individual healthcare information that is stored or transmitted electronically.

HIPAA requires standards for both security and privacy. The two are distinct but related. The health information security refers to the protection of a system from unauthorized access, whether external or internal. Privacy, on the other hand, refers to the individual's right to confidentiality of personal information. Privacy assumes the protection of security. Privacy requires security policies, security procedures, and security practices to ensure that the right to privacy is adequately protected.

The HIPAA standards are technology neutral. They have no effect on which electronic format you use to store individual healthcare information as long as you are able to convert it to the required format for electronic data interchange between healthcare entities. The standards also allow businesses to choose the technology that is most suitable for their specific needs. Thus there can be competitive solutions that will comply with HIPAA and offer business advantages for different healthcare organizations.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Main Requirements of the Security Standards

There are four primary requirements of the HIPAA security standards: Information Systems Security; Physical Security; Audit Trails; and Digital Signatures and Data Encryption.

- **Information Systems Security** deals with the protection of computers or workstations used to view, transmit, and store patient medical data and related information. This protection must cover both internal and external threats. Meeting security requirements in this area may include internal audits, personnel security, virus checks, incident procedures, termination procedures, risk analysis, access lists, security policies, and password management.

- **Physical Security** refers to the protection of buildings and information assets from any security threat, preventing unauthorized access to the workstations, network, or storage facility. Access codes, backup and storage, sign-in logs, door locks, secure databases, and protection of multiple points of entry in a network are critical.

- **Audit Trails** are required to monitor activities that relate to individual health information. This includes documentation of actions taken with the information and the personnel involved.

- **Digital Signatures and Data Encryption** provide requirements for transmissions to be authenticated and protected from observation or change. These measures will safeguard the integrity of health information as it passes through intranets, extranets, and the Internet.

HIPAA also includes an electronic signature standard that is not necessary for compliance. However, if a healthcare entity elects to use electronic signatures for healthcare transactions, then it must comply with the HIPAA electronic signature standard.

In the area of information systems security, one of the most important elements is the management of access to information. The HIPAA security standard, at section 142.308(c)(1)(i)(B), requires the use of either

1. user-based access control,
2. role-based access control or
3. context-based access control.

Although many applications will support any of these access control schemes, some legacy systems or applications will provide limited options. The decision of which scheme to use must be made, in part, on the administrative overhead. Healthcare entities must manage that access control system through all the staffing changes the organization experiences. In the nursing home industry, this is of particular concern because the employee turnover is high.

So careful consideration must be given to the overhead required to manage several access control methods that might apply to different systems. While a sophisticated database system might

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

support context-based access control, many legacy applications will need to use role-based or user-based controls. Most organizations will have to choose between the administrative complexity of supporting several access control methods and the benefits of using similar control methods across several applications or systems.

There are many tools available that might help to automate the process of managing access lists for systems or networks. Operating systems generally provide default user-based access management. Some of the newest versions support both user- and role-based control (e.g., Microsoft's Windows 2000 Active Directory). There are also many access management products available that can be added to the operating environment to automate these functions and add enhancements. Several of these directory products support role-based access controls. Examples include Nortel's Access Policy Manager and OpenNetworks' DirectorySmart for Microsoft's Active Directory.

Role-Based Access Control (RBAC)

Role-based access control (RBAC) is considered by many information managers to be the best method for establishing, controlling, and tracking network access. It is becoming a standard way to manage access for major directory services. In a RBAC system

- "Roles" are created that correspond to the organization's structure.
- Each "role" is then assigned a set of access privileges that are the minimum required for an employee with that role to do his or her job.
- Each employee in the organization is then assigned one or more roles that determine their level of network access.

RBAC Benefits

There are a number of benefits to using RBAC over user-based access control. Essentially, the RBAC scheme will grant access to an individual only if that person has been assigned the appropriate role or responsibility in the organization. All rights assignments are made by "role" in an RBAC environment. With user-based access control, each privilege must be granted to the individual user needing that access. In organizations with hundreds of systems and thousands of users, this can easily be overwhelming to administer. Some of the most important benefits of the RBAC system include

- RBAC simplifies access definitions, auditing, and administration of security access rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- By not assigning rights directly to individual users the delegation of access rights does not occur at the discretion of any user, even the security administrator. Roles are clearly defined and imposed, with no exceptions.

- Users are given only the access privileges necessary to perform their duties or role. This cuts down on intentional or inadvertent viewing, deletion, or modification of files.

- Updates can be done to roles (which apply to multiple users) instead of updating privileges for every user on an individual basis.

Context-based access control schemes have most of the same benefits as RBAC. They also allow an additional layer of control. In the case of a healthcare environment, this means that a context-based system can manage the question of privilege for a particular user who has the appropriate role and has been authorized by the particular patient whose record is being accessed. This additional capability automates the process required by HIPAA. However, this type of control is not available for all environments or applications. The availability of the RBAC scheme will often make it the preferred choice for access control.

Once the control scheme has been selected, implementation must be carefully planned to ensure successful operation. It must begin by developing a clear and understandable procedure that can be followed by both users and administrators. Then all administrative functions and tools must be protected from inappropriate use. The administrative tasks must also include careful monitoring of changes in staff or their roles. Finally, there must be an auditing procedure to verify the actions of the security administrator.

Develop a Clear Procedure

The security administrator is potentially the weakest link. Therefore the access control policies and procedures must be clear, complete, and religiously adhered to by the security administrator (and everyone else with user ID add/modify/delete authority) to protect the integrity of the system.

- Lay out the policy and procedures for access requests that meet the specific needs of the organization.

- Establish an approval policy for modification to the user management policy and procedures (change management).

- Establish an approval policy for user ID requests (appropriate authorization for actions).

- Set out a firm timeline for all changes. For example, policy and procedure changes could be effective immediately after approval. User ID access changes might be effective within 3 to 5 working days, but no later.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Secure Your Administrative Functions

All products, tools, and utilities used to administer your network and control access should be physically and electronically protected. Create a list of all such tools and systematically check them manually. This should be reviewed regularly and audited electronically, if possible.

Watch Personnel Changes

Notification of promotions, re-organization, departures, and terminations are the key obstacles to controlling access. A near-zero response time to such changes must be in place to ensure that there are no security gaps. Be sure not to overlook changes in the security administration staff. The most significant vulnerabilities are:

- Individuals who are no longer employees (particularly if they are disgruntled for any reason).
- Individuals who need different access to fill a new position. They should not be left with their old access privileges when the new rights are granted.
- Individuals granted temporary access for projects, but no longer require it. Any temporary access rights should include a firm cancellation date.

Establish an Auditing Procedure

A policy is only as good as the degree to which it is followed. Auditing compliance must be done on a regimented schedule. In particular, the security administrator's activities should be audited and any policy exceptions should be tracked. Ultimately, the goal is to know who did what, when, and how for every access transaction.

Conclusion

Role-based access control is a valuable tool that can be used to comply with HIPAA security requirements. Proper implementation can simplify the task of handling a high volume of security-related transactions. Taking the time to properly plan and implement a robust access control scheme will satisfy the HIPAA security standard and allow the organization's management to sleep soundly at night.

REFERENCES

Branco, Marcia. "Overview of HIPAA's Security Concepts". SANS Institute, April 13, 2000. URL: http://www.sans.org/infosecFAQ/legal/HIPAA.htm

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Cassidy, Bonnie. "HIPAA: Understanding Requirements". *Journal of the AHIMA*, April 2000.
URL: http://www.ahima.org/journal/features/feature.0004.3.html

Fagin, Daniel. "HIPAA Security Standards". SANS Institute, August 10, 2001.
URL: http://www.sans.org/infosecFAQ/standards/HIPAA_sec.htm

Ferraiolo, David and Kuhn, Richard. "Role-Based Access Controls". National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, Gaithersburg, MD. Originally published in the Proceedings of the 15th National Computer Security Conference, Vol II, pp 554-563, 1992.
URL: http://hissa.ncsl.nist.gov/rbac/paper/rbac1.html

Ferraiolo, David, Cugini, Janet, and Kuhn, Richard. "Role-Based Access Control (RBAC): Features and Motivations". National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, Gaithersburg, MD. Originally published in the 11th Annual Computer Security Applications Proceedings, 1995.
URL: http://hissa.nist.gov/rbac/newpaper/rbac.html

HHS Press Office. "Protecting the Privacy of Patients' Health Information". *HHS Fact Sheet*, May 9, 2001.
URL: http://aspe.hhs.gov/admnsimp/final/pvcfact2.htm

Institute for Health Care Research and Policy. "Summary of New Federal Health Privacy Regulations". Georgetown University, Washington, DC, January 2001.
URL: http://www.hipaadvisory.com/action/privacy/summaryreg.htm

Lebkicher, Michael. "Role Based Access". SANS Institute, November 30, 2000.
URL: http://www.sans.org/infosecFAQ/securitybasics/RBAC.htm

Public Law 104-191, AUG 21, 1996, Health Insurance Portability and Accountably Act of 1996
URL: http://aspe.hhs.gov/admnsimp/nprm/sec09.htm

Smith, Harry. "A Context-Based Access Control Model for HIPAA Privacy and Security Compliance". SANS Institute, July 18, 2001.
URL: http://www.sans.org/infosecFAQ/legal/control_model.htm

Tomes, Jonathan. *The Compliance Guide to HIPAA and the HHS Regulations*, Veterans Press, Overland Park, KS, 1999.

U.S. Department of Health and Human Services. "Security and Electronic Signature Standards; Proposed Rule" *The Federal Register*, 45 CFR Part 42, August 12, 1998.
URL: http://aspe.hhs.gov/admnsimp/nprm/seclist.htm

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Vasquez, Wiley. "Enterprise Security Administration: System and Application Access Management Exposures and Vulnerabilities". SANS Institute, October 4, 2000.
URL: http://www.sans.org/infosecFAQ/securitybasics/ESA.htm

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.