An Audit Report on

Security Over Electronic Protected Health Information at Selected Texas Academic Medical Institutions

November 2002

Report No. 03-009

State Auditor's Office

Lawrence F. Alwin, CPA
State Auditor

An Audit Report on

Security Over Electronic Protected Health Information at Selected Texas Academic Medical Institutions

SAO Report No. 03-009
November 2002

Overall Conclusion

System access and security control weaknesses at some Texas academic medical institutions have the potential to place electronic protected health information at risk. Individuals both inside and outside these medical institutions could gain unauthorized access to automated systems and read, copy, and possibly modify and delete electronic health information. Intruders also could disrupt the operations of systems that are critical in providing health care. In addition, the disaster recovery plans and physical security for information systems may not be adequate to prevent emergencies and natural disasters from causing significant disruptions to critical systems.

Protected Health Information

Protected health information includes individually identifiable health information (including demographic information collected from an individual) that relates to any of the following:

- The past, present, or future physical or mental health or condition of an individual
- The provision of health care to an individual
- The past, present, or future payment for the provision of health care to an individual

Protected health information directly identifies an individual or provides a reasonable basis to believe that the information can be used to identify an individual.

Source: Texas Health and Safety Code, Chapter 181

Academic medical institutions use and collect an extensive amount of protected health information for the purposes of student education, research, patient care, and public service. Unauthorized access to or alteration of this information could result in substantial financial losses from the assessment of federal and state civil penalties, lawsuits, and erosion of consumer confidence.

This report provides a general summary of the system access and security, disaster recovery, and physical security weaknesses we identified at selected academic medical institutions. To minimize the risks associated with public disclosure, this report does not include the institutions' names or reveal specific vulnerabilities that could further jeopardize the confidentiality of electronic patient health information. We have provided the medical institutions we audited with detailed information describing the specific vulnerabilities and recommendations for correcting them.

Summary of Management's Reponses

The academic medical institutions we audited generally agree with our recommendations. They have provided detailed plans, time lines, and names of staff members who are responsible for addressing their respective issues.

State Auditor's Office
Lawrence F. Alwin, CPA
State Auditor

This audit was conducted in accordance with Government Code, Section 321.0133.

For more information regarding this report, please contact Ron Franke, Audit Manager, at (512) 936-9500.

Summary of Information Technology Review

This audit was limited to selected information systems that contain confidential protected health information. We also reviewed the access and security controls for systems that authenticate users and allow general access to networks, e-mail, and the Internet. We did not examine the accuracy of the data in any system or review the controls over the institutions' major accounting or human resource systems.

We conducted network scans at selected academic medical institutions to identify vulnerabilities present in the systems we audited. Using Internet Security Systems' Internet Scanner™, we identified high-, medium-, and low-risk vulnerabilities. These scans were limited to agreed-upon network areas and did not cover all areas of the medical institutions' networks.

Detailed Results

Introduction

Academic medical institutions generally have four-part missions: student education, research, patient care, and public service. In fulfilling their missions, these institutions generate, collect, and exchange protected health information such as patients' diagnoses, lab results, and treatment histories. They also collect sensitive financial information (such as insurance billing records and social security numbers) that any other business might maintain. Failure to protect this information from unauthorized access or modification could expose these institutions to substantial financial losses from the assessment of federal and state civil penalties, lawsuits, and erosion in consumer confidence.

Incidents in other states illustrate what can happen when protected health information is not adequately protected:

- In New York, a Congresswoman's confidential medical records were faxed to reporters four weeks before her first congressional election in 1992.[1]
- A hacker successfully copied files containing information about 5,000 University of Washington Medical Center patients. The hacker used passwords from a server that was not secure to access thousands of files related to patients in the medical institution's cardiology and rehabilitation departments.[2]

The risks of unauthorized access to or modification of protected health information are increasing as more information is being stored and exchanged electronically. Couple the increasing use of electronic information with the fact that academic medical institutions are highly decentralized organizations, and the risks grow even larger. Many departments within medical institutions have their own budgets and independently acquire, develop, operate, and maintain their networks. While this decentralized approach allows for greater flexibility, it complicates a medical institution's ability to implement and enforce standard security measures to protect health information. The varying sizes of medical institutions' information technology security staff and security budgets also have an impact on these institutions' relative ability to address information security concerns.

Academic medical institutions in particular face a significant risk that intruders will be motivated to hack into their systems and use their extensive computing resources for unauthorized purposes. Because more intrusion or hacking tools have become readily available, even an unsophisticated hacker can download tools from the Internet and simply point and click to hack into automated systems.

Unauthorized access to or modification of protected health information can have a damaging effect on medical institutions' reputations. Maintaining their standing is

[1] Alissa J. Rubin, "Records No Longer for Doctors' Eyes Only," *Los Angeles Times*, 1 September 1998, p. A1.

[2] Marc L. Songini, "Hospital Confirms Copying of Patient Files by Hacker," *ComputerWorld*, 18 December 2000, p.7.

important in ensuring that medical institutions continue to receive research funding and preserve their customer base and associated revenue.

The federal government has tightened the legal requirements regarding the protection of health information. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) established specific health information protection requirements with which medical institutions must comply, including protecting health information from unauthorized uses or disclosures. If medical institutions do not comply with these requirements, they could be subject to financial penalties (see text box).

Penalties for Violating HIPAA Regulations

Civil Penalties:

- Not more than $100 for each violation, with a maximum of $25,000 per year.

Criminal Penalties:

- Wrongful disclosure offense - $50,000, imprisonment of not more than one year, or both.
- Offense under false pretenses - $100,000, imprisonment of not more than 5 years, or both.
- Offense with intent to sell information - $250,000, imprisonment of not more than 10 years, or both.

Source: Health Insurance Portability and Accountability Act of 1996

Protecting electronic records requires more effort than simply locking file cabinets. Achieving adequate protection requires an institution to allocate resources so that it can retain qualified technical staff and purchase necessary hardware and software. Protecting electronic records may also require a change in philosophy on the part of hospital staff, researchers, students, and other users. All of these individuals must become more cautious about how they store and exchange protected health information. Making the required change in resource allocation and philosophy depends on executive management’s full understanding of the risks and consequences of inadequate network security.

The institutions we audited were already aware of many of the system access and security control weaknesses we identified. Each of these institutions is in various stages of developing and implementing plans to improve information security; however, some actions are dependent on resource availability.

Chapter 1

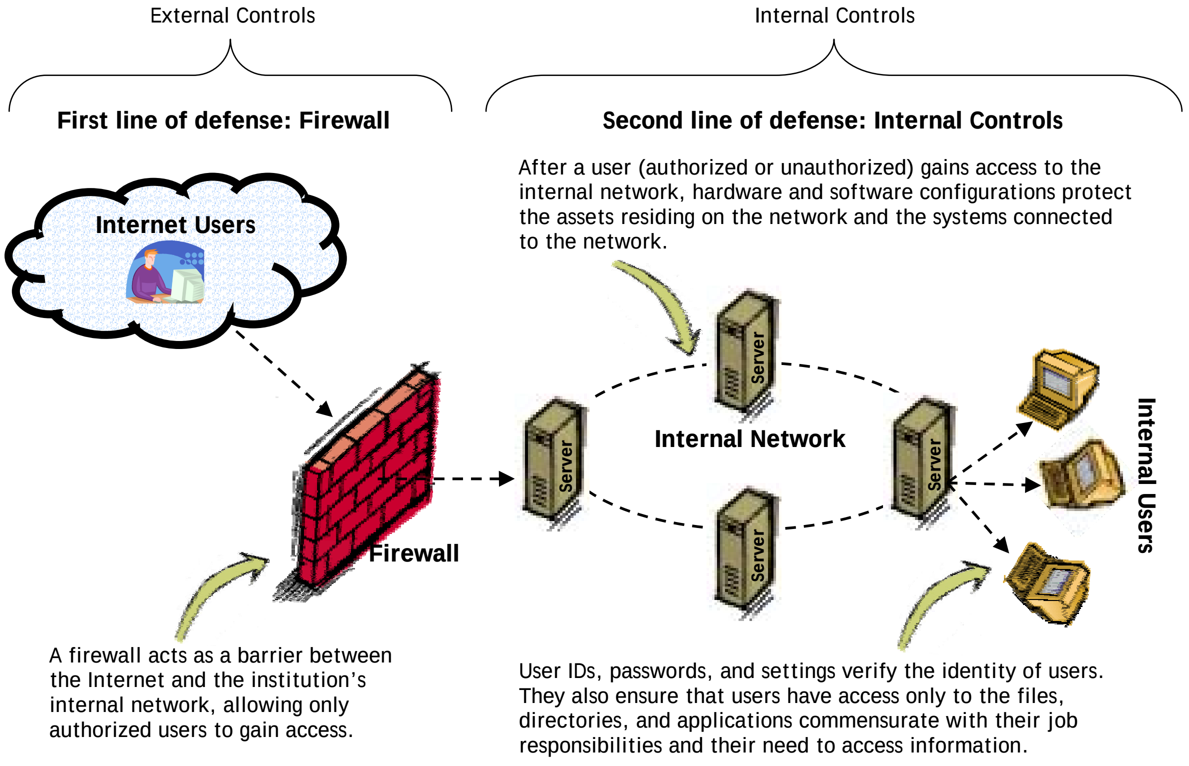
Access and Security Controls May Not Adequately Protect Health Information

Some academic medical institutions we audited lack effective firewalls to prevent external attacks and unauthorized access to the network. These institutions also lack internal system controls that would protect internal network resources and mitigate the risks associated with ineffective firewalls. To protect confidential information, these institutions must focus on both internal and external threats.

As Figure 1 shows, access and security controls are important in both preventing an attack from outside a medical institution through the Internet and controlling the resources and information available to users within the institution.

Figure 1 — Simplified Illustration of Network Security

Access and security controls are important in both preventing unauthorized access from outside the institution, especially through the Internet (external controls), and controlling access to the resources and information available to users within the institutions (internal controls).



After a user (authorized or unauthorized) gains access to the internal network, hardware and software configurations protect the assets residing on the network and the systems connected to the network.

A firewall acts as a barrier between the Internet and the institution's internal network, allowing only authorized users to gain access.

User IDs, passwords, and settings verify the identity of users. They also ensure that users have access only to the files, directories, and applications commensurate with their job responsibilities and their need to access information.

Security starts with protecting the network at the perimeter, where the internal network connects to external networks and the Internet, usually through a firewall. A firewall filters information to allow appropriate access and deny inappropriate access to the internal network.

When there are weaknesses in an external firewall, internal system controls become increasingly important to protect internal network resources. Internal system controls include proper configurations of hardware and software to prevent unauthorized access and external attacks. They also include user IDs and passwords, as well as settings that define the information resources users can access. These controls also manage access within a network. The fact that most of the damage from unauthorized access is caused by internal users (rather than external hackers) makes internal system controls even more important in protecting network resources.

Chapter 1-A

Medical Institutions' Controls May Not Effectively Block Unauthorized Access

Some medical institutions' firewalls may not prevent unauthorized access from outside the institution. Some medical institutions that we audited do not have effective firewalls to prevent an external intruder from gaining access to critical internal systems and information stored on those systems. Although we did not attempt to exploit the vulnerabilities, our scans found high-, medium- and low-risk vulnerabilities. The medical institutions we audited have prepared detailed plans that would improve the security of their networks, especially to protect them from unauthorized external access attempts. These plans are in various stages of implementation, with some actions dependent on resource availability.

What Is a Firewall?

A firewall is a system of components that:

- Controls access between two networks, such as a private local area network (LAN) and the relatively more unsafe, public Internet.
- Determines which inside services can be accessed from the outside.
- Allows access to authorized users.
- Denies access to unauthorized users.

Source: Information Security Standards, Texas Administrative Code, Title 1, Chapter 202

Internal system controls at the academic medical institutions may not effectively block unauthorized access to some information systems. We found critical systems within the medical institutions that do not have sufficient internal controls to prevent unauthorized access to confidential information or to prevent system failure resulting from malicious attacks. For example, certain systems that contain protected health information (medical evaluations, lab results, and billing records) have inadequate or blank passwords, are not configured securely, and have users assigned with inappropriate levels of access. As a result, the protected patient health information on these systems and any connected system is at risk.

Examples of the internal system control weaknesses we identified include the following:

- System settings for some medical institutions' systems that could allow extensive access through vulnerabilities. Our internal scans and on-site reviews identified high-, medium-, and low-risk vulnerabilities in certain systems. The types of internal system vulnerabilities identified could expose systems to denial-of-service attacks or the unwanted installation of computer viruses or other malicious applications.

- Lack of formal, consistent processes for installing software updates that fix vulnerabilities on all the computer equipment across the institutions. It is critical that the medical institutions address vulnerabilities on every system because the presence of a vulnerability on any one system attached to a network places the entire network and all interconnected systems at risk.

- Passwords that are blank, that can be guessed, or that are identical to the user IDs. The combination of a user ID and a password is one of the most common tools used to verify a user's identity and to control access to computer resources. If unauthorized users can determine the appropriate combination of a user's ID and password, they can log into a system with all of the access rights and capabilities of that user. Therefore, password vulnerabilities create significant risks that unauthorized users could gain inappropriate access to systems and information.

- Some users of the medical institutions' systems who have access to information that they do not need to perform their jobs. If high-level user permissions are not tightly restricted or correctly managed, a user could gain unnecessary access to sensitive information and systems. In addition, an intruder using that user's account could gain this same level of access.

  The medical institutions we audited are beginning to improve security by issuing certain users physical identification tools, such as smart cards or keys to the computers, that are used in addition to user IDs and passwords. These additional tools may reduce the risk that an intruder could use another person's user ID and password to gain network access.

Recommendations

We encourage all medical institutions to:

- Ensure that their external access controls are in place and are configured to address vulnerabilities that could allow an intruder to gain unauthorized access.

- Continue to implement their security plans and work with executive management to obtain necessary resources.

- Develop and implement a consistent process for installing software updates to address the identified security risks.

- Strengthen and enforce password policies.

- Examine system configurations to ensure that proper user permissions are set.

Chapter 1-B

Inconsistency in Logging System Activities and in Reviewing Logs Prevents Effective Intrusion Detection

While the major systems at the medical institutions we audited create logs to capture system activity information such as system traffic, processing errors, and access attempts, the medical institutions do not consistently retain and review these logs or analyze security incident trends from these logs. This is partly because the medical institutions lack a clear definition of a security incident that requires further investigation and have no documented policies on how to investigate these incidents. In addition, we found some systems that do not create logs to monitor system activity.

When system logs are not created, maintained, and reviewed, system administrators may not be able to detect an intrusion or other unauthorized actions or be able to act promptly to minimize the impact of an intrusion. In addition, users may be less likely to commit unauthorized activities if they know that their actions are being recorded in logs.

Recommendations

Medical institutions should:

- Evaluate systems to ensure that appropriate logging functions are enabled and establish and implement policies and procedures for log retention.
- Establish and enforce procedures for reviewing system logs.
- Develop and implement procedures for analyzing security incident trends and use this analysis to improve system security.
- Develop and implement policies that define a security incident and procedures for investigating potential incidents.

Chapter 1-C

Inadequate User Access Management Could Allow Former Employees to Access Systems

While the medical institutions follow formal processes to remove user network access, these processes may not ensure that the institutions promptly remove access rights as soon as employees leave the institutions or change positions. For example, one institution updates employee access rights on a weekly basis. As a result, an employee who leaves the institution at the beginning of this process could retain access rights for a full week. In addition, these formal processes may not remove network access rights for temporary users (such as contract employees, vendors, or visiting faculty) for whom information is not recorded in major human resources or student information systems.

These institutions grant and remove access to independent systems and data at the department level using an even less formal process. Administrators of these independent systems do not always receive notification of employee termination and do not review user access to these systems on a regular basis. These weaknesses could allow former employees and temporary users to have access after they no longer need it.

Recommendation

Medical institutions should improve processes to ensure the timely removal of user access to their systems when users leave the institutions, especially for temporary users such as contract and temporary employees, vendors, and visiting faculty.

Chapter 1-D

Inadequate Planning May Prevent Timely Compliance With HIPAA Regulations

While the Texas Administrative Code requires all state agencies to implement security controls over information resources, HIPAA regulations, though not completely finalized, specifically require medical institutions to ensure the security and privacy of protected health information. The institutions we audited are implementing plans for compliance with HIPAA regulations; however, one institution is just beginning to address its compliance and may have difficulty meeting compliance deadlines (see text box).

Violations of HIPAA regulations could subject the medical institutions to penalties ranging from $50,000 for wrongful disclosure of health information to $250,000 and 10 years imprisonment for wrongful disclosure with the intent to sell information. However, the consequences of violating HIPAA regulations go beyond financial penalties. HIPAA violations could ultimately affect a medical institution’s ability to remain accredited, putting its insurance reimbursement status at risk.

HIPAA Compliance Deadlines

Electronic Transaction Standards - October 16, 2002 (Institutions may apply for a one-year extension)

Establishes standard data content, codes, and formats for submitting electronic claims and other administrative health care transactions.

Privacy Standards – April 14, 2003

Limits the use and release of protected health information; restricts most disclosure of health information to the minimum needed for the intended purpose; and establishes safeguards and restrictions regarding disclosure of records for certain public responsibilities.

Security Standards – Standards Not Final

Protects electronic health information systems from improper access or alteration.

Source: Health Insurance Portability and Accountability Act of 1996

Recommendations

Medical institutions should:

- Ensure that their efforts to comply with HIPAA regulations enable them to meet compliance deadlines.

- Coordinate with similar institutions that have already conducted significant HIPAA planning to share policies and procedures, user training, and other tools to ensure compliance.

Chapter 2

Technology Disaster Recovery Plans May Not Ensure Timely System Recovery

Medical institutions' information technology disaster recovery plans may not be comprehensive enough to minimize the business impact and to ensure the timely resumption of service in the event of a disaster or other disruption of its information systems. The Texas Administrative Code, Title 1, Chapter 202 (Information Security Standards), requires state entities to prepare disaster recovery plans. These plans are important in minimizing the effects of a disaster on information resources and in ensuring that the institutions will be able to either maintain or quickly resume critical functions.

We found the following components missing in some medical institution disaster recovery plans:

- Time frames for recovery and arrangements for acquiring replacement equipment after a disaster occurs
- Documented management procedures for assessing the adequacy of the disaster recovery plan and updating the plan after a disaster
- Provisions for executive approval of plan updates
- Plans for annual testing

Recommendations

Medical institutions should:

- Establish and document a prioritized plan for the restoration of critical systems and applications that also includes time frames for recovery and arrangements for acquiring replacement equipment.
- Specifically state in the disaster recovery plan the frequency of plan updates and reviews and include a requirement for executive management sign-off on the updates and reviews.
- Develop and document in the disaster recovery plan post-disaster review and wrap-up procedures to assess the adequacy of the plan and update the plan following a disaster or emergency.
- Document procedures for annual testing of disaster recovery plans.

Chapter 3

Some Network Resources Are Not Adequately Protected

While the medical institution data centers that house major network and system hardware are generally physically secure, other information resources and network cabling are not adequately protected from damage or theft.

Not all equipment and electronic information is protected from loss. While the medical institutions generally have adequate environmental controls that protect the computer equipment from fire, heat, and water in their major data centers, other locations where they store important network or computer equipment are not adequately protected. For example, equipment purchased by individual departments is sometimes stored in a locked office with no special environmental controls.

In addition, the medical institutions do not always require users to store information on the central servers. This makes controlling and protecting potentially sensitive information more difficult. It also increases the risk that this information could be lost if a computer were lost or damaged because data on individual computers may not be backed up on a regular basis.

Exposed cabling risks disruption of communication. We found instances in which network and communications cabling is exposed to public access. At one institution, the cabling is not protected from fire and is easily accessible through public doorways. At the other institutions, fiber-optic cabling is exposed to limited public access outside the institution. The direct exposure and accessibility of network and communications cabling increases the risk that these cables could be damaged by natural disasters, accidents, or intentional actions, resulting in disruption of voice and data communication.

Recommendations

Medical institutions should:

- Ensure that network and communications cabling is enclosed and secure to prevent public access.
- Place servers with protected health information in secure locations with appropriate environmental controls.
- Require users to store critical or confidential information on the central servers rather than on their personal laptop or local computers.

Chapter 4

The Risks Associated With Wireless Technology Require Further Study

Many medical institutions, including the ones we audited, are experimenting with wireless technology because of its low cost, user mobility, and associated increases in productivity. However, the results of our testing indicate that the institutions had active wireless devices that management had not approved. In addition, we were able to capture unprotected information transmitted through these wireless devices. This indicates that the institutions should place greater emphasis on identifying and securing access points to their wireless networks.

While wireless technology is rapidly expanding, security for wireless technology has not developed as quickly. Wireless local area networks pose an increased security risk because they send information via radio waves, not through physical wires. Radio waves generally travel farther than the physical limits of a building, and as a result, information could be captured without detection by network security personnel. With the right equipment, a hacker within the proper range can transmit data to a wireless access point or capture and read information stored on a wireless network. In addition, the entire network may become vulnerable to unauthorized access from wireless access points inappropriately installed inside an institution’s firewall.

Recommendation

We encourage all institutions to create and enforce wireless security policies and to educate users about the risks of using wireless technology.

Other Information

Objectives, Scope, and Methodology

Objectives

The objectives of the audit were to determine whether the medical institutions:

- Have adequate access and security controls for the major health information management systems to ensure that critical protected health information is sufficiently protected from loss or misuse.
- Have developed and tested disaster recovery plans to ensure that emergencies and natural disasters will not cause significant disruptions to health information management systems.

Scope

The scope of the audit included the major systems that contain protected health information at selected academic medical institutions.

Methodology

The audit methodology consisted of interviewing staff, reviewing disaster recovery and information security plans and policies, inspecting major data centers, and conducting internal and external network scans to identify potential system vulnerabilities.

Project Information

We conducted fieldwork from April 2002 through July 2002. We conducted this audit in accordance with generally accepted government auditing standards.

Distribution Information

Legislative Audit Committee

The Honorable James E. "Pete" Laney, Speaker of the House, Chair
The Honorable Bill Ratliff, Lieutenant Governor, Vice Chair
The Honorable Rodney Ellis, Senate Finance Committee
The Honorable Florence Shapiro, Senate State Affairs Committee
The Honorable Robert Junell, House Appropriations Committee
The Honorable Rene O. Oliveira, House Ways and Means Committee

Office of the Governor

The Honorable Rick Perry, Governor

In compliance with the Americans with Disabilities Act, this document may also be requested in alternative formats. To do so, contact Production Services at (512) 936-9880 (Voice), (512) 936-9400 (FAX), 1-800-RELAY-TX (TDD), or visit the Robert E. Johnson Building, 1501 North Congress Avenue, Suite 4.224, Austin, Texas 78701.