

HIPAA Security Seminar Outline

Bill Ganucheau, MA, MBA, CMPE
WRG001@LAPHYSCORP.COM

Spring, 2001



Seminar Presenter

Bill Ganuchau is Director of Information Systems for Louisiana Physician Corporation. He holds an MBA from the University of Louisiana at Lafayette, and is credentialed as a Certified Medical Practice Executive in the Medical Group Management Association (MGMA). Louisiana Physician Corporation provides on-line shared systems and full practice management services for over 100 medical practices in Louisiana and Mississippi.

Part 1. Introduction

Benefits of connectivity and decentralization

Information decentralization and incremental user empowerment have been driving information systems development for twenty years in all industries. Health care is no exception. Certainly, no one who has known the benefits of networked information systems, Internet email, bulletin boards, discussion groups, or broadband Internet access would want to return to the days of single-function dumb terminal access to a centralized internal health care information system. Online connectivity to broader health care systems and to the Internet has greatly accelerated the pace of information processing and has boosted productivity. However, these advances in connectivity and productivity also put information systems at risk as never before.

A balancing act: security is the antithesis to connectivity

- A security system which is too stringent—or badly implemented—will barricade legitimate users from resources and impeded productivity
- Too lax a system will expose health care organizations to very serious threats
 - Privacy violations
 - Legal and liability exposure
 - Damaging public relations
 - Data corruption or loss
 - System down time due to external attacks

HIPAA regulations: standards for protecting health care information

- Balance between efficiency and privacy
- Standardization of code sets vs. rights of individuals to privacy

The HIPAA benefit/cost trade-off

- Major benefits will come from standardized transaction codes sets
 - Major costs will come from implementing privacy and security regulations
- ❑ **The purpose of this seminar**
- Review proposed HIPAA security requirements
 - Discuss internal vs. external threats
 - Describe the vulnerabilities and protections for current technologies
 - Outline an overview of a model for continuous security monitoring and improvement
 - Provide additional resources to participants
 - ❑ HIPAA Security Glossary
 - ❑ Annotated security bibliography

The seminar is not intended to be a “blueprint” for HIPAA compliance, but rather to aid practices in achieving that compliance by defining the proposed regulations, and exploring risks and safeguards associated with specific information technologies.

Anyone with even a little technology background can lose an audience in acronyms and jargon. My intention is to bring you along with me, not to see how quickly I can lose you.

Part 2. Security Strategies

Stand-alone, terminal-based information systems of old required little more than physical protection for the host system and login/password controls. Today’s integrated and networked information systems—often with “always-on” Internet connectivity—can be attacked by an anonymous hacker half a world away. To adequately protect today’s health care information systems, controls and defenses must be substantially more robust. The extent and cost of these defenses will vary greatly with the size of the organization, and the level of information technology deployment.

- ❑ **Introduction to HIPAA security regulations**
- Proposed regulations only, at this time
 - Timeline for compliance
 - Penalties for non-compliance
 - Regulations are written to be “technology neutral”
 - Also written to be scalable

- Result is often ambiguous regulations without sufficient specificity
- Enterprise-wide security...not just a technology issue

Highlights of HIPAA Security Implementation Categories

The HIPAA (proposed) regulations describe four categories of security implementation requirements: Administrative, Physical, Technical Services, and Technical Mechanisms. Each of these categories will be reviewed briefly here. There is overlap among these divisions, because (1) each category level builds upon the safeguards of the lower levels; and (2) many technology implementations require administrative components in order to work. Security is an continuous, organization-wide priority; it is not simply a matter of installing the right hardware and software!

(Figure 1)

- **Administrative Procedures**
 - Login and password control and management
 - Who authorizes new logins?
 - Termination procedures
 - Security training and reminders
 - Periodic security audits
 - Security incident procedures
- **Physical Safeguards**
 - Media controls
 - Perimeter security
 - Secure workstation location
 - Security awareness training
 - Resource protection

- Backup and disaster recovery
- Technical Security Services
 - Access control
 - User identification
 - Data Authentication
 - Biometrics
- Technical Security Mechanisms (if a computer network is implemented)
 - Access control
 - Audit trail
 - Event reporting
 - Entity authentication

Overlap in HIPAA categories

- Many technical or physical controls require administrative implementations as well.
 - Media controls
 - Incident procedures
- Overlap serves to prevent perception of security as strictly a “technology” issue
 - A login procedure featuring passwords which are encrypted with the latest technology can’t prevent a user from sharing a password with a co-worker.
 - The best firewall in the world won’t prevent a user from infecting a network with a virus from an email attachment or diskette.

- A recurrent theme is the need for security training and reminders.
- Policies and technical implementations must be supported by a zero-tolerance violation policy, where every security violation by users is followed by an appropriate sanction.
 - Establishing a secure modem pool may not prevent users from bypassing the pool and establishing modem connections through a local fax port; but the threat of punishment might do so.

Part 3. Detailed Review of Security Regulations

Sources for the following table, itemizing the HIPAA security regulations and Questions/Issues:

- “HIPAA Security Summit Guidelines (Draft).” (26 Jun. 2000). Online. Internet. 10 Jan. 2001. Available <http://www.smed.com/hipaa/draft.pdf> .
- United States. Department of Health and Human Services. “Notice of Proposed Rule Making for the Security and Electronic Signature Standards.” Cong. Rec. 12 Aug. 1998. 43241-43280. <http://aspe.os.dhhs.gov/admnsimp/nprm/seclist.htm>
- University of Missouri Health Care. “HIPAA Security Standards: Definitions.” (01 Mar. 2000). Online. Internet. 5 Jan. 2001. Available <http://hsc.missouri.edu/~hipaa/reference/hpra09.html> .

Administrative Procedures

HIPAA Requirement	Implementation	Questions and Issues
<p>Certification</p> <p><i>The technical evaluation performed as part of, and in support of, the accreditation process that establishes the extent to which a particular computer system or network design and implementation meet the HIPAA security requirements. This evaluation may be performed internally or by an external accrediting agency.</i></p>		<ul style="list-style-type: none"> ❖ What are the baseline goals for certification? The regulations don't stipulate standards! ❖ Do we have the resources to self-certify? ❖ Presumably, organizations like JCAHO and NCQA will offer certification processes.
<p>Chain of trust partner agreements</p> <p><i>A contract entered into by two business partners in which it is agreed to exchange data and that the first party will transmit information to the second party, where the data transmitted is</i></p>		<ul style="list-style-type: none"> ❖ How will we identify all of our business partners? ❖ Can we utilize existing agreements? ❖ How will we monitor compliance (our own, and that of our partners)? ❖ How will security breaches be reported? ❖ What will be the consequences of non-compliance (intentional vs unintentional)?

Administrative Procedures

HIPAA Requirement	Implementation	Questions and Issues
<p><i>agreed to be protected between the partners. Required between all parties who exchange electronic health information</i></p>		
<p>Contingency plan (all listed implementation features must be implemented).</p> <p><i>A plan for responding to a system emergency. The plan includes performing backups, preparing critical facilities that can be used to facilitate continuity of operations in the event of an emergency, and recovering from a disaster.</i></p>	<ul style="list-style-type: none"> – Applications and data criticality analysis – Data backup plan – Disaster recovery plan – Emergency mode operation plan – Testing and revision 	<ul style="list-style-type: none"> ❖ Is there a designated person responsible for contingency planning? ❖ Have systems and applications been ranked for continuity priority? ❖ What is the frequency and scope of regular backups? Are they stored off-site? ❖ Have backups been tested for full restoration? ❖ Are backup and restoration procedures fully documented? ❖ Is there already a disaster recovery plan in place, which can serve as a starting point? ❖ Is there a documented, tested process for implementing down-time procedures, including the decision criteria for invoking those procedures?
<p>Formal mechanism for</p>		<ul style="list-style-type: none"> ❖ What process exists to govern the creation of health

Administrative Procedures

HIPAA Requirement	Implementation	Questions and Issues
<p>processing records</p> <p><i>Documented policies and procedures for the routine, and non-routine, receipt, manipulation, storage, dissemination, transmission, and/or disposal of health information.</i></p>		<p>information, and how is that information validated for accuracy?</p> <ul style="list-style-type: none"> ❖ What processes exist for determining who shall have the authority to change or manipulate data once created, and what audit trails exist to log such changes? ❖ What policies exist to govern how long data will be stored prior to being archived or destroyed? ❖ What policies and procedures are in place to protect data transmitted internally and externally? ❖ What policies are in place to ensure that health information is disposed of securely, including destruction of media containing health information?
<p>Information Access Control</p> <p><i>Formal, documented policies and procedures for granting different levels of access to health care information</i></p>	<ul style="list-style-type: none"> _ Access authorization _ Access establishment _ Access modification 	<ul style="list-style-type: none"> ❖ Access Control Lists (ACL) and role-based access systems are most comprehensive methods. ❖ Do we currently have a documented access control policy? ❖ Does our policy cover the entire organization, including all sites, departments, and corporate entities? ❖ Does the access policy cover on-site as well as remote access?

Administrative Procedures

HIPAA Requirement	Implementation	Questions and Issues
		<ul style="list-style-type: none"> ❖ What mechanism will be instituted to grant access to health information on all media, electronic and paper? ❖ Is access authorization level documented and maintained for each employee, physician, researcher, volunteer, temp employee and contractor? ❖ Are ALL systems and applications containing health information subject to the same access authorization controls?
<p>Internal Audit</p> <p><i>On-going, internal review of the records of system activity (for example, logins, file accesses, security incidents).</i></p>		<ul style="list-style-type: none"> ❖ Many systems and applications in use today do not include audit logs and audit trails. ❖ Many that do include audit logs don't have sophisticated reporting modules (i.e. mountains of data, and no way to spot outliers).

Administrative Procedures

HIPAA Requirement	Implementation	Questions and Issues
<p>Personnel Security</p> <p><i>Policies and procedures to ensure that all personnel (including agents and subcontractors) who have access to health information have the required authorities and clearances to do so.</i></p>	<p>_ Assure supervision of maintenance personnel by authorized, knowledgeable person.</p> <p>_ Maintenance of record of access authorizations</p> <p>_ Operating, and in some cases, maintenance personnel have proper access authorization</p> <p>_ Personnel clearance procedure</p> <p>_ Personnel security policy/procedure</p>	<ul style="list-style-type: none"> ❖ Do policies exist for oversight of maintenance and operating personnel working in the vicinity of health information, or on information systems? ❖ Will criminal background checks be required as a prerequisite to hiring or granting access privileges? ❖ Have applicants and current employees been checked against the OIG sanctions list? ❖ What process exists to ensure that employees and contractors sign agreements which delineate individual security responsibilities and accountability for maintaining confidentiality? Is there a recertification process for these agreements? ❖ Are systems users, including maintenance and operating personnel trained in security? Are third parties with access to organizational systems included in the security training process?

Administrative Procedures

HIPAA Requirement	Implementation	Questions and Issues
<p>Security Configuration Management</p> <p><i>Policies and procedures to ensure security integrity across multiple platforms, applications and systems.</i></p>	<ul style="list-style-type: none"> _ Documentation _ Hardware/software installation and maintenance review and testing for security features _ Inventory procedures _ Security testing _ Virus checking 	<ul style="list-style-type: none"> ❖ Do security measures for all information systems exist? ❖ Are security measures for disparate systems coordinated? If so, how? Single-login procedure? ❖ Are new applications tested for security prior to roll-out? ❖ Is a physical inventory maintained and kept accurate and current of all hardware and software assets in the organization? ❖ Is security testing—including intrusion testing—performed regularly on systems and networks? ❖ Are virus checking procedures in place and utilized? ❖ What is the reporting and response process when viruses are detected? ❖ Is virus checking software kept current to ensure trapping of new viruses?

Administrative Procedures

HIPAA Requirement	Implementation	Questions and Issues
<p>Security Incident Procedures</p> <p><i>A formal process to deal with identifying, reporting and responding to real or potential intrusions or security policy violations.</i></p>	<p>_ Report procedures</p> <p>_ Response procedures</p>	<ul style="list-style-type: none"> ❖ Does the security policy differentiate between serious and non-serious incidents? ❖ Does the security policy include handling of viruses? ❖ Does the security policy assign responsibility for handling incidents? ❖ Does the security policy address the issue of timeliness in investigating and reporting security incidents? ❖ Does the security policy include procedures for reporting of findings of security incidents, corrective action taken, recommendations, and follow-up? ❖ Does the security policy include coordination with local and federal law enforcement agencies?
<p>Security Management Process</p> <p><i>An on-going process to manage security risks involving creating, administering, and overseeing policies to ensure the prevention, detection, containment,</i></p>	<p>_ Risk analysis</p> <p>_ Risk management</p> <p>_ Sanction policy</p> <p>_ Security policy</p>	<ul style="list-style-type: none"> ❖ Is there a process for ongoing assessment of effectiveness of control measures and for identifying and responding to problem trends? ❖ Are employees required to read and sign security and confidentiality agreements? ❖ Are there specific sanctions for specific types and levels of violations? ❖ Is there consistent enforcement?

Administrative Procedures

HIPAA Requirement	Implementation	Questions and Issues
<p><i>and correction of security breaches.</i></p>		<ul style="list-style-type: none"> ❖ Is the security policy comprehensive, covering all business and technical areas, systems, communications and storage media, and all affected personnel, both internal and external? ❖ Does the security policy cover exception and emergency access procedures? ❖ Does the security policy set forth standard or accepted tools, products or methods for key security areas such as firewalls, encryption, electronic mail and Internet usage? ❖ Are security training and awareness programs required by the security policy? ❖ Does the security policy cover backup and recovery procedures?
<p>Termination Procedures</p> <p><i>Formal, documented procedures to revoke user access when an employee terminates employment, to prevent unauthorized access by former</i></p>	<ul style="list-style-type: none"> _ Changing combination locks _ Removal from access lists _ Removal of user account(s) _ Turn in of keys, tokens, or cards that allow access 	<ul style="list-style-type: none"> ❖ Is there an employee termination policy in place? ❖ Are responsibilities clearly defined and understood? ❖ Is a communication protocol in place to address timing/timeliness of termination procedures between Human Resources and Information Systems functions?

Administrative Procedures

HIPAA Requirement	Implementation	Questions and Issues
<p><i>employees.</i></p>		<ul style="list-style-type: none"> ❖ Does the policy distinguish between employee- and employer-initiated termination? ❖ Is an exit interview conducted in which potential security concerns are identified, documented and acted upon? ❖ Is there assigned responsibility for signing off termination process in each case?
<p>Training</p> <p><i>Security training must be provided for all staff regarding the vulnerabilities of the health information in an entity's possession, and procedures which must be followed to ensure the protection of that information.</i></p>	<ul style="list-style-type: none"> _ Awareness training for all personnel, including management _ Periodic user reminders _ User education concerning virus protection _ User education in importance of monitoring login success/failure, and how to report discrepancies _ User education in password management 	<ul style="list-style-type: none"> ❖ Is there a formal organizational security training program? ❖ Is there an annual or more frequent re-certification process in place for employees' security training? ❖ How does the training program support various classes of system users and the level of information sensitivity to which they have access? ❖ Are all system users included in the training program, including those employees and non-employees accessing organizational systems from remote sites? ❖ Does the security training program include education regarding protection against and reporting of viruses, identifying potential security breaches, and managing individual passwords?

Administrative Procedures

HIPAA Requirement	Implementation	Questions and Issues
<p>Assigned Security Responsibility</p> <p><i>Responsibility for health information security must be assigned to an individual or organization.</i></p>		<ul style="list-style-type: none"> ❖ Has a security officer been designated, or has that function been assigned to an outside agent? ❖ Does that security officer or agent have sufficient authority to manage and oversee the security controls and processes?
<p>Media Controls</p> <p><i>Formal, documented policies and procedures that govern the receipt and removal of hardware/software media (disks, diskettes, tapes, optical media) into and out of a facility.</i></p>	<ul style="list-style-type: none"> _ Accountability _ Data backup _ Data storage _ Disposal 	<ul style="list-style-type: none"> ❖ Is there a logging procedure to account for the introduction, removal and destruction of all media? ❖ Is there a policy governing employee-introduced media (disks, CD-ROMs)? ❖ Are backups performed daily, and stored securely off-site? ❖ Are data servers in secure, locked locations? ❖ Is there a retention schedule which covers all data, stipulating on-line, off-line, and destruction timetables? ❖ Is the media/data destruction process secure? ❖ Are data on workstations as well as central servers protected from unauthorized access by passwords or access control lists?
<p>Physical Access Controls</p>	<ul style="list-style-type: none"> _ Disaster recovery 	<ul style="list-style-type: none"> ❖ Is there a disaster recovery plan, itemizing procedures

Administrative Procedures

HIPAA Requirement	Implementation	Questions and Issues
<p><i>Policies and procedures to limit physical access to and within an entity, while ensuring that properly authorized access is allowed.</i></p>	<ul style="list-style-type: none"> _ Emergency mode operation _ Equipment control _ Facility security plan _ Procedures for verifying access authorizations prior to physical access _ Maintenance records _ Need-to-know procedures for personnel access _ Sign-in for visitors and escort (if appropriate) _ Testing and revision 	<p>to be followed in the event of physical damage to systems, data or facilities?</p> <ul style="list-style-type: none"> ❖ Is the organization prepared to operate temporarily without computer systems, or with minimal system resources? ❖ Is all equipment identified? ❖ Are all equipment moves, repairs, and disposals logged? ❖ Is there a facility security plan in place, with procedures to follow in the event of fire, power failure, catastrophic weather, or physical intrusion? ❖ Are maintenance records maintained for computer equipment? ❖ Are visitors and maintenance personnel required to sign in? Are they given temporary identification? Are they escorted? ❖ Have disaster recovery procedures (data restore, etc.) been tested?
<p>Policy/guideline on Workstation Use</p> <p><i>Policies describing</i></p>		<ul style="list-style-type: none"> ❖ Is there a policy on proper work station use? ❖ Does the policy include important security issues such as password control and privacy and the importance

Administrative Procedures

HIPAA Requirement	Implementation	Questions and Issues
<p><i>proper use of work stations, appropriate functions, and login/logoff procedures</i></p>		<p>of logging off of work stations when tasks are complete.</p>
<p>Secure Workstation Location</p> <p><i>Workstations must be located in such a way to prevent unauthorized access to health information.</i></p>		<ul style="list-style-type: none"> ❖ Are workstation screens shielded from the view of patients and other visitors? ❖ Are workstations in public areas protected from unauthorized access by password-protected screen savers or other access controls?
<p>Security Awareness Training</p> <p><i>Security awareness training required for all employees. (See Administrative Procedures, above)</i></p>		
<p>Access Control</p> <p><i>Controls must be in place to restrict access to resources to authorized individuals and entities.</i></p>	<p>_ Procedure for emergency access</p> <p>One of the following must be used:</p>	<ul style="list-style-type: none"> ❖ Is there a process for screening unwarranted demands for access? ❖ Do systems allow for individual user ID's and passwords? ❖ Are there different levels of access based on users'

Administrative Procedures

HIPAA Requirement	Implementation	Questions and Issues
	<ul style="list-style-type: none"> _ Context-based access _ Role-based access _ User-based access <p>Optional:</p> <ul style="list-style-type: none"> _ Encryption 	<p>specific job requirements?</p> <ul style="list-style-type: none"> ❖ Does the system log sign-on events? Who reviews them? ❖ Are there access log reporting or alert capabilities? ❖ Although encryption is not required, are best practices followed in encrypting passwords?
<p>Audit Control</p> <p><i>Records of login activity, which can be examined for suspect data access activities.</i></p>		<ul style="list-style-type: none"> ❖ Are current systems capable of producing reports to review an audit trail of system access? ❖ Do systems have the ability to produce an alarm based on unauthorized access? ❖ Is there an alarm for unusual/inappropriate login activities with volume thresholds? ❖ Is authentication strong enough to identify someone for disciplinary action? ❖ What is the retention period for audit logs?
<p>Authorization Control</p> <p><i>Maintain mechanisms for</i></p>	<p>One of the following is required:</p> <ul style="list-style-type: none"> _ Role-based access 	<ul style="list-style-type: none"> ❖ Are group logins prohibited? ❖ Do login systems allow mapping back to an

Administrative Procedures

HIPAA Requirement	Implementation	Questions and Issues
<p><i>obtaining consent for the use and disclosure of health information. (The login/password or other access/authentication scheme will accomplish this for online users.)</i></p>	<p>_ User-based access</p>	<p>individual?</p> <ul style="list-style-type: none"> ❖ Are passwords changed on a regular basis? Can the system force periodic password changes? ❖ Is disclosure of passwords explicitly forbidden?
<p>Data Authentication</p> <p><i>Organizations are required to guarantee that data in its possession has not been altered or destroyed in an unauthorized manner.</i></p>	<p>Examples of methods:</p> <ul style="list-style-type: none"> _ Check sum _ Double keying _ Message authentication codes _ Digital signatures 	<ul style="list-style-type: none"> ❖ See “Formal Method for Processing Records” in Administrative Procedures ❖ What data authentication means are employed when transmitting to/from an outside entity?
<p>Entity Authentication</p> <p><i>Organizations are required to verify that trading partners and users are—in fact—who they say they are.</i></p>	<p>One or more of these mechanisms should be used:</p> <ul style="list-style-type: none"> _ Automatic log off _ Unique user identification _ A biometric identification system _ A password system 	<ul style="list-style-type: none"> ❖ Does the capability exist to authenticate entities communicating with our organization? ❖ If passwords are used, are minimal “strong” password conventions employed? (i.e. minimum of 6 characters; common dictionary words disallowed; combination of letters and numbers; changed at least every 6 months; passwords cannot be the same as user ID’s or logins) ❖ If passwords are used, are “cracker” programs run at

Administrative Procedures

HIPAA Requirement	Implementation	Questions and Issues
	<ul style="list-style-type: none"> _ A personal identification number (PIN) _ Telephone call back _ A token system which uses a physical device for user identification 	<p>least twice a year to evaluate the strength of user passwords?</p> <ul style="list-style-type: none"> ❖ If tokens are used (i.e. smart cards) are they only accepted with a user-entered PIN for system access?
<p>Communication Network Controls</p> <p><i>Organizations that use communications or networks are required to protect health information transmitted electronically, so that they cannot be easily intercepted by parties other than the intended recipient; they must also protect their systems from intruders.</i></p>	<ul style="list-style-type: none"> _ Encryption (required in open networks; optional in private-wire arrangements) _ Integrity Controls _ Message Authentication <p>One of the following must be implemented:</p> <ul style="list-style-type: none"> _ Access controls _ Encryption <p>If using a network, the following 4 implementation features must be in place:</p>	<ul style="list-style-type: none"> ❖ Is continuous intrusion monitoring in place on the network? ❖ Does monitoring include alarms so that immediate action can be taken, if necessary? ❖ Are there documented procedures to follow for security event reporting? Are there escalating types of events described? ❖ Is there an assigned responsibility to monitor Internet sites providing information about new threats, viruses and malicious code? ❖ Are all business partners required to use access controls when accessing systems? ❖ What methods (integrity controls; message authentication) are used to ensure data are transmitted and received accurately between business partners?

Administrative Procedures

HIPAA Requirement	Implementation	Questions and Issues
-------------------	----------------	----------------------

	<ul style="list-style-type: none"> _ Alarm _ Audit trail _ Entity authentication _ Event reporting 	<ul style="list-style-type: none"> ❖ Is encryption technology available for open network transmission of health information data? Is there an Internet usage policy, covering the use of electronic mail?
--	--	--

Part 4. Internal Security Threats

Although most of the media focus and attention with respect to computer security is on external threats, health care organizations should not underestimate internal threats. These may be either intentional or unintentional, malicious or mindless. Protecting information systems from internal security threats is as important as erecting an impenetrable external physical perimeter security system. “I have seen the enemy, and he is me!” (**Figure 2**)

❑ **Hiring and training**

- Background checks?
- Security training integrated into new-hire procedures
- Security reminders

❑ **User computer knowledge and sophistication**

- Can't rely on user ignorance for security
- The trend to decentralize information continues, making it increasingly difficult to erect a “glass wall” around corporate information.
- Assignment of appropriate access or privilege levels (and monitoring changes to those privilege levels) is vital
- As personal computers more and more replace dumb terminals as workstations, users find themselves at the command of a very powerful interface to the corporate information systems.
- Users are increasingly savvy about networks, the Internet, and protocols such as *TCP/IP* (the Internet protocol), *telnet* (for remote system login) and *ftp* (the file transfer protocol used widely in networked systems).

❑ **Malicious intent**

- Disgruntled workers have more powerful tools at their disposal, as well as connectivity to multiple systems
- Terminated employees are often privy not only to their own logins and passwords, but possibly phone numbers for modems, IP addresses, etc.
- The Internet *does* have a dark side, and it doesn't require too much determination for a person intent on inflicting harm to seek out and find malicious code, techniques and methods to attempt to launch an attack on a targeted organization.

Part 5. Security Threats and Defenses—an Overview

When an aircraft carrier puts out to sea it is protected by battleships and destroyers all around it on the surface, submarines below the surface farther out, and a 24-hour aircraft patrol farther out still. This system of erecting perimeter barriers in concentric circles around an important asset can be used to visualize the security barriers required for health care information systems. A particular health care organization may require only some of these perimeter defenses, depending on the level of connectivity and exposure. As the level of interconnectivity increases, so does the cost and complexity of securing the information assets which are placed in the hands of users. There are four broad categories of controls needed. Each of these information technology (I.T.) implementations will be discussed in more detail below, as well as the corresponding threats and countermeasures which must be erected in each instance. As with the aircraft carrier group, each level of controls protects against different threats, but lower-level controls often support, enable, or enhance the high-level controls. This overview presents each of the control categories, to place the subsequent detailed coverage in a larger perspective. **(Figure 3)**

- Physical controls**
- Modem controls**
- LAN controls**
- WAN and Broadband Internet controls**

Part 6. Physical Controls

- Central Information Systems**
 - I.T. Implementation
 - Practice management systems
 - Electronic medical records (EMR) systems
 - Scheduling or registration systems
 - Security threats

- Unauthorized physical access
- Physical disaster
- Data corruption
- Countermeasures
 - Physical barriers
 - People
 - Data backup
 - Off-site backup storage
 - Disaster recovery plan
 - Criticality analysis
 - Contingency plans
 - Disaster recovery team

Terminal-Based Multi-User Systems

- I.T. Implementation
 - Single-function terminals
- Security threats
 - Public access to terminal screens
 - Disgruntled employees
 - Terminated employees
 - Login/password sharing or compromise
- Countermeasures

- Physical security for terminals
- Security training and reminders
- Termination procedures
- Access & authorization controls
- Workstation use policy

Part 7. Modem Controls

Dedicated Point-to-Point Connection

- I.T. Implementation
 - Dedicated analog leased lines for remote site access
 - Dedicated digital leased lines for remote site access
- Security threats
 - Phone tap (local or at phone company)
- Countermeasures
 - Security warning/notice at login
 - Modem, CSU/DSU, and multiplexor configuration
(A modem is the hardware which enables digital communication over analog phone lines; a CSU/DSU performs the same function for digital lines; a multiplexor enables multiple users on either analog or digital data lines to share the same connection.)
 - Encryption

Remote Dial-in via Modem

- I.T. Implementation
 - Physician access from home

- Tele-commuters
- Remote site access
- Remote-control software
- Support modem for system vendor dial-in
- Security threats
 - Unauthorized external dial-in
 - Phone tap
- Countermeasures
 - Automatic call-back modem for physician home access and remote site access
 - Automatic call-back from different modem in modem pool
 - Support modem kept off-line when not in use
 - Strong authorization control for remote-control PC (personal computer) access
 - Termination procedures to prevent access to known modem numbers

Electronic Data Interchange (EDI) via Modem

- I.T. Implementation
 - Dial-up connectivity with business partners
 - Transmission of health claim, remittance advice, pre-certification, eligibility, laboratory, and prescription data
- Security threats
 - Unauthorized external dial-in
 - Phone tap

- Countermeasures
 - Automatic session termination
 - Disable modem auto-answer on host side
 - Time-of-day controls
 - Encryption

Dial-up Internet Access

- I.T. Implementation
 - Personal computers
 - World Wide Web browser
 - Internet email
 - File and program downloads
- Security threats
 - Exchange of patient information via Internet email
 - Viruses, worms and Trojan horses
 - Data corruption or destruction
- Countermeasures
 - User education in computer virus threat
 - User education in patient privacy
 - Anti-virus software
 - Frequent data backup
 - Frequent virus software updates

- Encrypted email

Part 8. LAN Controls

Local Area Network

- I.T. Implementation
 - Multi-function PC workstations
 - File and resources sharing (printers, modems, fax)
 - Corporate Intranet
- Security threats
 - Computer viruses
 - Prying eyes
- Countermeasures
 - Media controls & policy
 - Turn off sharing of hard drives
 - Protect sensitive files with passwords
 - Network operating system to authenticate user identification & permissions
 - Monitor software vendor web sites for patches to fix software vulnerabilities
 - Hardware Inventory control procedures, especially for laptops

Remote Network Dial-in

- I.T. Implementation
 - Physician access to network resources, EMR system, or scheduling system
 - Telecommuters

- Security threats
 - Unauthorized dial-in
- Countermeasures
 - Strong user identification and authorization procedures
 - Encryption
 - Termination procedures to deny future access to remote user

Part 9. WAN and Broadband Internet Controls

Broadband Internet Access

- I.T. Implementation
 - “Always on” Internet access
 - Fast, multi-user Internet access
- Security threats
 - Unauthorized external access to system
- Countermeasures
 - Firewall
(Hardware/software which only allows authorized users access to a system)
 - Intrusion detection system
(Software that detects unusual activity or unauthorized access to a system, and issues an alert to the administrator)
 - “Probing” software to test strength of firewall
 - Internet usage policy

Wide Area Network

- I.T. Implementation

- Frame relay network
- Virtual private network (VPN)
- Public switched technology

- Security Threat

- Unauthorized access or packet monitoring
- Permanent Virtual Circuits (PVCs) reveal pre-defined “route,” if intercepted
- TCP/IP protocol sometimes used for vendor management functions, which can expose the network to penetration
- Port scanning attack
(In this kind of attack, a hacker searching for “back door” into systems— at random or by targeting a particular system)

- Countermeasures

- Strong vendor relationship
- Firewall
- Intrusion detection system
- Encryption

World Wide Web Hosting

- I.T. Implementation

- Corporate WWW site (information, policies, procedures, forms)
- Email connectivity to patients

- Links to health related sites
- Appointment scheduling
- Patient prescription refill requests
- FTP server
(File Transfer Protocol server; usually a host machine which allows anonymous users to log on and download files to their system)
- Application Service Provider (ASP)
(An ASP offers on-line services to clients over the Internet.)

- Security threats

- Denial of service attacks
(The network is flooded with dummy or duplicate email traffic or requests for information, causing it to slow down or stop, thus denying service and resources to legitimate users.)
- Spoofing
(A hacker obtains login/password information, and logs on, impersonating a legitimate user.)
- Port scanning *(defined above)*
- False webs
(A hacker lures a user on the World Wide Web to access what appears to be a legitimate site, and once there, all of that user's data for the duration of the session, passes through the hacker's site before reaching it's destination; thus the hacker is able to monitor all data—passwords, credit card numbers, etc.)
- Compromise of Intranet via web server
(If proper controls are not in place, a hacker can use the web server as a portal to access internal servers and data.)

- Countermeasures

- Separate host machine for web server
- Firewall
- Positive patient identification system for email and prescriptions
- Email encryption
- Intrusion detection system

Part 10. HIPAA Security On-Going Monitoring and Reporting

No security system will remain effective unless it is reviewed and modified in a continuous improvement cycle. The following model presents a framework for this process (**Figure 4**).

Organization controls

- The controls used to protect health information are one of three types:
 - Management

 - Operational

 - Technical

- The combination of these controls DO overlap, but that overlap is necessary. (For example, if user administration is weak, and unauthorized users are given legitimate logins and access, the technical controls in place to challenge users with logins and passwords will not prevent these unauthorized users from gaining access.)

Continuous monitoring and periodic review of controls

- Once the controls are in place, a system must be developed to monitor and review those controls
- This ensures that the controls are still working properly
- Some controls (like 24x7 firewalls and intrusion detection systems) must be monitored constantly;
- Other controls (like termination procedures and security training) can be handled effectively through periodic reviews and audits.
- In developing such a model for monitoring and review, the following issues must be address:
 - Timing: When and how often should reviews of each control occur? What activities or events should trigger a review?

- Tools: What software audit tools are needed for continuous monitoring? What reports or logs are needed for periodic reviews?
- Personnel: Will additional personnel (or fractional FTE's) be required to perform continuous monitoring and periodic reviews?
- Skills: Are there special technical skills or training required to implement and use monitoring systems, or to generate required audit logs? (i.e. programming to spot outliers in audit data, or to automate generation of logs)

Reporting and Documentation

- Compliance with HIPAA security regulations will require ongoing documentation—not just a one-time fix like the Y2K bug.
- Some reports will be needed to perform audits, others to certify ongoing compliance.
- For each report, the following must be determined:
 - which reports are needed;
 - the appropriate level of detail (detail, department; executive summary)
 - the type of documentation needed to prove the specific control is effective, and that it was reviewed;
 - a retention schedule for the report;
 - the timing of the report: continuous; periodic; triggered by an event or security incident

Feedback, Change and Incorporation

- Over time, we can expect controls to become less effective. This is because:
 - technology changes rapidly, and today's bullet-proof security techniques will be compromised tomorrow by superior technology or ever-inventive maliciousness;
 - software upgrades, and incremental addition of software tools, hardware platforms and connectivity methods often introduce gaps in overall security.
- In order to combat the degradation of system security, the on-going review process as well as new system additions are evaluated for security vulnerabilities. When discovered, this feedback is used to design changes in system security. These changes are integrated into the basic controls (technical, operational and management).
- Then the iterative process begins again, with the new controls in place.
- The bottom line for the organization is the need to get feedback from the monitoring and review process, and incorporate changes into the existing

security infrastructure. This may include changes to to controls themselves as well as changes to the monitoring and review process.

Part 11. Conclusion

- “Never use the words ‘computer’ and ‘secure’ in the same sentence”**
- The cost of security–how much is enough?**
- Today’s airtight controls will be insufficient tomorrow**
- Need for constant vigilance, testing and improvement**

Part 12. Additional Resources

- HIPAA Security Glossary**
- HIPAA Security Annotated Bibliography**