Appendix D:
IT Privacy and Security Primer

PART 1:
GENERAL PRIVACY CONSIDERATIONS[1]

Introduction

The purpose of this IT Privacy and Security Primer is to provide a broad overview of what privacy in health care represents. This section is not intended to address the state and federal legal requirements related to the privacy of identifiable health information, which are covered in Appendix C, *Relevant Legal Requirements for Health Data Exchange for Health Care Organizations.*

Privacy is something many working in the field of health care take for granted. There is an understanding that all those working in the field of health care know that a patient or plan member's personal health information is to be kept confidential and only used to serve the best interests of the patient or plan member. It has become part of the culture, whether health plan or provider.

Unfortunately, some segments of the health care industry have misused patient or plan member information or not established the safeguards that prevent access to it by those who are not authorized to view the confidential health information. This has resulted in more restrictive federal and state laws, legal action, and reputation damage to certain organizations.

The Health Insurance Portability and Accountability Act (HIPAA) clearly defines how patient and plan member information is to be treated and what the exceptions are regarding release without patient or plan member authorization. State and federal law other than HIPAA provides further guidance regarding the release or restrictions on release of patient or plan member information by identifying specially sensitive information. Legal requirements, though, represent the floor and not necessarily all of the privacy protections that an organization may choose to adopt or should adopt. In other words, organizations can go above and beyond the law providing greater protections than state or federal laws require.

There are three standards that need to be adhered to when developing an appropriate privacy program—integrity (information accuracy), confidentiality (preventing the wrong person from accessing or using the data), and availability (the data are accessible when needed by appropriate parties). While law defines requirements related to the treatment of confidential information, organizations are responsible for implementation of such safeguards. If nothing else, integrity, confidentiality, and availability are key to the success of any privacy (and security) program.

[1] Chris Apgar, CISSP, Apgar and Associates, LLC.

Different and sometimes conflicting business practices have been adopted to address maintaining and managing individually identifiable health information. Some are based on the actual requirements of state and federal laws, some are based on identified organizational needs (as defined by the organization) and some are defined by lack of knowledge regarding legal requirements and what is considered appropriate privacy practice.

As an example, a provider may adopt a practice of not exchanging any identifiable health information without the patient's consent. This provides additional protection to the patient but interferes with appropriate medical treatment. It is important to remember that the purpose of privacy is not to completely wall off confidential data, either between departments within an organization or between an organization and the outside world. An effective privacy program or privacy practice allows the use of confidential information while implementing policies, procedures, and practices that keep confidential data out of the hands of individuals not authorized to see it (in other words, those who have no legitimate need to view the confidential information).

The movement toward electronic health records and regional health information exchange increases the risk of inappropriate access to identifiable health information but can help improve health care quality, lower costs, and prevent medical errors. Absolute, risk-free privacy (and security) may not be attainable; instead, patient and plan member benefits must be balanced against these risks. Developing common privacy standards that are followed by the health care industry may provide that balance.

The construction of a viable privacy program, especially if it involves multiple organizations, depends on developing common standards, common forms, common methods of exchanging information, and proper protections of that information. Creating a community health record, for example, does not mean privacy and security must be compromised. Instead, it means that information users must agree on how information is handled, protected, and exchanged. Again, privacy risks may increase, but those risks can be managed to ensure that they are outweighed by the benefits to the patient or plan member.

Sharing information between organizations requires a workable audit program and periodic risk analysis. Action must be taken if it is found that an individual or entity has abused their privileges, advertently or inadvertently exposing identifiable health information, violating the agreed-upon standards of the organizations involved in the data exchange. Sanctions are required and must be enforced.

Within an organization, it is appropriate to clearly identify an individual's need to access information and to establish a role-based access program (a program that allows members of the workforce to view only the information they need to do their jobs). It is also necessary to implement appropriate risk analysis processes and audit processes within an

organization to make sure that information is not misused in violation of organizational policy and practice.

Below is a list of the areas that a role-based program should take into account, whether information is to be shared between organizations, such as via a community health record, or used internally within an organization. This list is not all inclusive. Areas of potential risk where clearly defined policies are needed include:

- marketing;
- fund raising;
- use for other than treatment, payment, and health care operations;
- requests by the patient or plan member to view or receive a copy of his or her medical or claims record
- requests for restriction by the patient or plan member;
- requests for amendment by the patient or plan member;
- requests for an accounting of disclosure by the patient or plan member, including any inappropriate releases of information;
- requests by the patient or plan member for alternate means of communication;
- authorization for release to a third party by the patient or plan member;
- state and federal laws more stringent than HIPAA;
- access control and management;
- authentication;
- auditing (specific and general);
- risk analysis and management;
- who "owns" the data;
- who is responsible for policy, procedure, and practice maintenance and enforcement, including training; and
- privacy incident investigation, mitigation, and follow-up.

Summary

Privacy amounts to adhering to the concepts of integrity, confidentiality, and availability. Privacy is not risk free but if an organization or a collaborative implements appropriate policies, procedures, and practices, these privacy risks will be outweighed by benefits to patients and plan members. Policies, procedures, and practices should ensure that only the *minimum necessary* individually identifiable data are shared except when used for treatment, that the data in all forms are protected, and that data are shared on behalf of the patient or plan member to meet their needs.

The purpose of privacy is to reasonably ensure confidential information is used and shared only when necessary or required by state or federal law (eg, law enforcement, public health,

and health care oversight). It is the responsibility of organizations (internally and externally) to ensure proper health care while not misusing data or risking exposure of data to entities or individuals not authorized to view that information.

PART 2:
ADMINISTRATIVE SECURITY[2]

Introduction

The purpose of this part of the IT Privacy and Security Primer is to address administrative security. For regulatory references, please see Appendix C. It has been long known in the security field that people and not technology represent the greatest risk to the establishment of appropriate security practices. No matter how robust security technical safeguards are, security may be compromised if the workforce is not aware of or disregards appropriate security practices. It is very important to not only establish appropriate security policies, procedures, and practices but also to clearly communicate them to and enforce them with the workforce, trading partners, and affiliated organizations. A well-designed training program can be an effective approach to informing the workforce regarding what is expected of them when performing assigned duties, whether internally or as it relates to accessing data through a RHIO or other type of HIE.

Risk Analysis and Follow-up (Risk Management)

The foundation of any sound security program is the risk analysis. A properly conducted risk analysis will assist in identifying areas where threats and vulnerabilities endanger the security of organizational information. It also forms the foundation for creating appropriate procedures, policies, and practices by clearly identifying in ranking order what needs to be addressed first. The results of the risk analysis will point to holes in an organization's security infrastructure that can often be addressed through policy and training.

There are three types of risk analysis—qualitative, quantitative, and rank order. Most organizations use the qualitative method because the other two methods are more cumbersome and, especially the quantitative method, involve sometimes complex calculations in determining risk. A solid resource that outlines risk analysis methodology can be found at the federal government's NIST web site, http://www.nist.gov. Risk assessment information is listed under the "800 series" of the NIST developed standards. The 800 series deals with appropriate security practices and processes.

Following a thorough risk analysis, an organization should have a list of threats and vulnerabilities and associated risks that should be addressed through policy, procedure, process, and sometimes new technology. The list and ranking of existing threats and vulnerabilities often point to holes in administrative practice which can be addressed through the development and/or amendment of existing policies, procedures, and practices. Not all of the threats or vulnerabilities identified during the risk assessment need to be addressed. As an example, if an identified risk is considered minor with minimal impact on the organization if it occurs, the organization may elect to note (documentation is

[2] Chris Apgar, CISSP, Apgar and Associates, LLC.

important) that the risk is negligible and the organization does not intend to address what are considered acceptable risks.

In addition to regulatory compliance, another benefit of a complete risk analysis is that it provides the starting point for developing a thorough risk management program. A risk management program is required by the HIPAA Security Rule (as is the risk analysis) and is considered sound security practice. The purpose of the risk management program is to develop a process where organizations can manage identified risks; monitor for new risks that may arise due to changes in business practice, technical infrastructure, or environmental factors such as new viruses; monitor the effectiveness of existing policies, procedures and practices; monitor and act on audit program results; and provide a sound starting point when preparing to conduct the next risk analysis (which should be conducted annually or when any major business or infrastructure changes occur). The risk management program is, in essence, establishing a watchdog over an organization's security program.

Auditing

Auditing is another process that is required by the HIPAA Security Rule. Most applications and hardware create audit logs that track activity within an organization's hardware and software infrastructure. This includes technical audit logs that track, as an example, firewall activity. It also includes tracking activity of workforce members when accessing, transmitting, modifying, creating, and destroying what is considered critical data to the organization, such as patient medical record information.

Every organization needs to establish a thorough audit program. This relates back to the risk analysis. The risk analysis results can be used to develop a part of the criteria to be evaluated by the internal auditor or audit team. It is important to periodically review the status of efforts to mitigate or eliminate identified threats and vulnerabilities. It is also important to review policies, procedures, and practices to reasonably ensure they are being followed and determine whether revisions are needed to better address business and security needs.

Another important component of any audit program is to review more frequently those areas that are considered critical to an organization. As a rule, most organizations complete a full audit on an annual basis. Organizations with an electronic health record (EHR) may wish to perform additional, random audits on access, record viewing, and modification of PHI.

It is important to know what audit logs are available in hardware and software used in an organization's environment. As an example, does the EHR create an audit record when a workforce member accesses the EHR? It is important when creating an audit program to identify which audit logs need to be activated and how any logs generated will be reviewed,

which audit logs should not be activated and why, and how to address situations where PHI is handled where there are no audit logs available (such as with legacy systems and when working with paper records).

Turning on all audit logs is generally not an effective practice unless the organization intends to look (at least randomly) at all audit logs created. The activation of unneeded audit logs creates two things: extra paper or electronic records that take up space but have no value (because they are not being looked at) and, second, a legal liability. If an audit log records, say, an inappropriate disclosure of PHI and that audit log is not reviewed, it can later be claimed in a civil suit that damages occurred related to the inappropriate disclosure that the organization had the information but failed to act on the information or demonstrate due diligence.

Audit programs should be managed by a member of the workforce who is relatively independent from the rest of the operational or technical parts of the organization. They need to have knowledge of the business but need to remain neutral when conducting audits. Also, the person managing the audit program should have at least a basic knowledge of appropriate auditing practices and related regulations.

One of the biggest mistakes organizations make is implementing an audit program but paying little or no attention to the reports generated following an audit. If a problem or issue is documented, the organization needs to, at the very least, document why the organization chose not to act on an audit finding. In most cases, the organization will need to take action through changes in policies, procedures, and practices, proceeding with appropriate sanctions if necessary and possibly modifying the technical infrastructure to addresses the issues identified in the audit report.

Policies and Procedures

Policies and procedures outline expectations for workforce members and subsidiary entities such as business associates and indicate how the organization intends to act regarding appropriate security management. Policies range from password management to authentication to transmission of data to use of e-mail and so forth. Policies and procedures also document adherence to regulatory requirements.

The difference between policies and procedures is that policies are generally high level and include statements of what the organization intends to do, including what is allowed and what is prohibited. Procedures outline in detail easy-to-follow steps that need to be taken to comply with the established policy. As an example, an organization may adopt what would be considered a strong password policy. The procedure would provide the details—the number of characters required, construction requirements (using alpha, numeric, and special characters), how frequently the password should be changed, and so forth.

Policies and procedures are necessary and required by the HIPAA Privacy and Security Rules. They are also required to address organizational business practices, sound security, and sound privacy practices. Policies and procedures are only as good as their enforcement. Policies and procedures need to be communicated to workforce members in an understandable way, and workforce members need to know that sanctions will result from noncompliance. Compliance needs to be monitored on a regular basis by management through the audit process and through ongoing risk analysis and good management.

Policies and procedures need to be reviewed on a regular basis, which is a regulatory requirement as well as sound business practice. Generally, this means policies and procedures should be reviewed annually or whenever a major business or system change occurs. It is also important to remember that if a policy is changed, the previous version needs to be maintained for a minimum of 6 years from the last day it was in effect. Annual risk assessments and audits will point out areas where policies and procedures need to be added or updated.

Training

Security programs are only as good as the knowledge level of the workforce charged with enforcing policies and following procedures. Also, general security concepts need to be communicated to the whole organization. The goal is to create what is called a security culture—where security becomes second nature and all members of the organization understand that appropriate security is important to the organization and the consumers they serve.

Creating a security culture requires initial general training (required by the HIPAA Privacy and Security Rules) that covers general security practices from the perspective of the organization. The HIPAA Security Rule is flexible and can be adapted to organizations of any size. When developing general security training, keep in mind the particular business practices of the organization. Security is meant to protect confidential information and the information technology (IT) infrastructure, but it also needs to accommodate the business needs of the organization.

General training needs to be reinforced through periodic security reminders. These can be short e-mails to all staff about a particular security practice, a refresher during a staff meeting, or a short article on the organization's intranet. One-time training is not adequate to reasonably ensure that the workforce is adhering to appropriate security practices. Security is an ongoing process. Training needs to be conducted with new workforce members, and specialized training may be needed for certain positions such as network engineers and health records managers.

When considering workforce security training, remember that "workforce" encompasses temporary employees, volunteers, and contractors who are not considered business

associates and have access to PHI. All need to be provided with at least summary security and privacy training. A two-sided form with security requirements on one side and privacy requirements on the other is usually sufficient. Individuals should sign the form indicating that they have read, understand, and agree to abide by the requirements, and the organization should retain the form to demonstrate that training was provided.

Members of the workforce need to be trained on the particular security policies, procedures and practices pertinent to their jobs. It is advisable to not merely hand the policy to affected members of the workforce but to also spend the time needed to walk through the policy, procedure or practice with a workforce member (or a group of members) and answer any questions. It is also necessary to provide updates to affected members of the workforce when policies, procedures, and practices change.

Disaster Recovery Planning/Emergency Mode Operations

Disaster planning can be built on the results of a thorough risk analysis. A complete risk analysis involves such things as identifying where data are stored, what protections are in place, what applications are in use, and what hardware has been implemented to support an organization's IT infrastructure. A disaster recovery plan uses that information to develop plans should some or all of the facility, IT infrastructure, or needed staff become unavailable. In other words, organizations need to determine how they will react to a natural disaster or fire, for example.

A disaster recovery plan needs to take into account the infrastructure needs (facility and IT) and staffing needs for critical business functions. A properly constructed plan will include which systems or portions of the operation will need to be "brought on line" first and identify workforce members responsible for reasonably ensuring that those functions are addressed in order of criticality. In addition to recovery of IT functions, a comprehensive disaster recovery plan needs to address plans for recovery of business operations, possible temporary staff deployment, and nontechnical ways of operating while systems are down.

Some organizations create what is called a "hot" site. A "hot" site is a location other than the main site that is fully functional and can easily accommodate the critical needs of the organization. Other organizations create a "warm" site: another location where all of the hardware and applications are available for use in the event of a disaster, but are not necessarily populated with the data needed for operations (which would be loaded from appropriate backed-up data). Another method of disaster planning is to create a "cold" site, which is a site at a different location that does not necessarily have all of the needed hardware and software but arrangements have been made with external vendors to supply the needed hardware and software, generally within hours in the event of a disaster.

Disaster recovery plans need to be flexible and continuously updated as members of the workforce move on to other positions or leave the organization. Specific individuals need to

be responsible for different parts of the disaster recovery plan to make sure updates are completed in a timely way. A disaster can happen at any time.

Development of a disaster recovery plan requires a review of critical activities within an organization and developing realistic plans to assist with recovery of those critical functions in the shortest possible period of time. Generally, disaster recovery plans are tiered—the most critical functions are addressed first, followed by tiers of functionality that are addressed in sequence to bring the whole organization back into pre-disaster condition.

Testing is another important component of disaster recovery planning. Testing can range from table top exercises to a full mock disaster. Tests should occur on a regular basis and can suggest ways to improve the plan to better address disasters should they occur.

The HIPAA Security Rule also requires organizations to establish emergency modes of operation. This closely relates to disaster recovery planning and implementation. In essence, an organization needs to identify critical functions and develop a plan to address critical functions, activities, and identified critical services. It is important to describe how the organization will operate under emergency conditions, even if it is only operating in triage mode (which would be the case, for example, if all health records were maintained in paper form and were destroyed by fire). Again, planning is essential. It is not possible to figure out how best to address the critical functions of the business such as patient care or claims processing while a disaster or emergency is occurring.

Sanctions

An appropriate sanctions policy and related procedure needs to be developed and implemented, probably in conjunction with an organization's human resources department. A sanctions policy demonstrates that the organization is serious about security, and that actions will be taken for violation of the organization's security policies, procedures, and practices (also a HIPAA Privacy and Security Rule requirement).

The sanctions policy needs to be clearly communicated to the workforce, including management. The policy needs to be adhered to, and actions taken need to be documented for HR reasons, for compliance reasons, and to demonstrate that sanctions are applied equally across the organization for violations of security. Generally, the sanctions policy is enforced by management in conjunction with human resources and is often based on audit log reports and other factors such as observing passwords that are written down and left in plain sight. The severity of the sanction should be tied to the severity of the violation. Violations should be documented before sanctions are imposed and, if pursuant to a security breach, documented by the incidence response team.

Security Incident Plans

All organizations covered under the HIPAA Security Rule are required to implement a security incident response plan. It is sound practice for entities not covered under HIPAA to develop a security incident response plan. The purpose of the plan is to assist the organization in rapidly responding to security breaches or suspected security breaches in an effort to limit damages, put processes/practices in place to prevent further incidents, and preserve evidence in the event the security breach is intentional. If law enforcement becomes involved, it is wise to preserve the evidence, especially as it ties the breach back to an individual. This helps protect the organization in the event that criminal or civil actions are taken later as a result of the breach.

Most security breaches occur from within an organization. It is important to protect the organization from outside threats such as hackers and viruses, but statistics show that the greatest percentage of breaches and associated damages originate from within the organization or the workforce. It is important to address potential breaches before they happen through training, appropriate policies, risk analysis, and so forth, but that will not necessarily prevent all security breaches from occurring. There is no such thing as a risk-free environment. The organization needs to be positioned to act quickly from a business, legal, and regulatory perspective.

Even though not required by the HIPAA Security Rule, organization should also implement a privacy incident response plan. The Privacy Rule includes what has been called a "mini-security rule" because security incidents become privacy incidents when they result in inappropriate disclosure of PHI.

Access to PHI

Applications and systems are generally configured so a user (an entity or individual) of an application or system is required to enter a form of unique identification before being allowed access to the application or system storing confidential data. This is generally a function of the technology but the technology is configured by people and access is initiated by a person.

It is wise to establish appropriate policies, procedures, and practices to reasonably ensure that:

- Access is authorized and managed.
- Access is monitored and modified as necessary (for example, when a workforce member moves to a different position).
- Users of systems and data are uniquely identified (critical to appropriate auditing).
- Access is controlled (workforce members have access to the minimum amount of confidential data necessary to do their job).

- The appropriate level of authentication is established and enforced to protect against inappropriate access by unauthorized individuals.
- Termination policies and procedures are in place to delete access by a workforce member when he or she no longer needs access or terminates employment. This is especially important when an employee is terminated involuntarily and includes termination practices associated with systems and facilities.

A number of organizations have implemented what is called role-based access. Role-based access means assigning access based on a workforce member's role or position in the organization. In some ways it is similar to a position description. A particular position is allowed access only to data needed to accomplish the duties of the position. It requires monitoring and changes. As an example, when a workforce member moves to a new position, the access privileges granted for the former position are revoked and the access privileges of the new position are established.

Role-based access does need to be flexible to accommodate special projects that may require additional access, a workforce member covering for another workforce member who is absent, and other contingencies. Also, the number of roles will depend on the size and complexity of the organization. Larger organizations generally need to define more roles. The organization needs to balance the number of roles it establishes with the time needed to manage role-based access. If too many roles are established (in other words, if too much granularity is defined), maintenance of roles becomes administratively burdensome. On the other hand, defining too few roles can defeat the purpose of role-based access.

The HIPAA Privacy Rule does not require adherence to *minimum necessary* standards if the release of information is for treatment purposes. Still, all members of the workforce do not need access to the complete medical record. The receptionist, as an example, does not need access to the complete medical record. He or she only needs access to the name of the patient, the time of the appointment, and often insurance coverage information. The receptionist does not need access to treatment plans and medication records.

Summary

This section merely serves as an example of some of the areas an organization needs to attend to when rolling out an appropriate security program. It is good to remember that security is more people-based rather than technology-based. The technology only works if backed by appropriate policies, procedures, and practices. Also, there are a number of areas that do not rely on technology for the dissemination of information (eg, faxing documents, telephone conversations, and hardcopy medical records).

The HIPAA Security Rule only covers electronic PHI. It is important to remember, though, that the Privacy Rule includes a security provision and the Privacy Rule applies to all PHI, no matter the form. Also, a sound security program will take into account PHI and other confidential data, regardless of the form.

PART 3:
PHYSICAL SECURITY[3]

Introduction

Physical security describes the broad category of safeguards that are designed to protect important information assets from a variety of threats, including theft, sabotage, and unauthorized intrusion. Physical security also comprises safeguards to protect electronic information systems, buildings, and equipment from natural and environmental disasters such as fire or flood. Such safeguards include the ability to quickly restore critical electronic information and operations following a disaster. In the context of health care, physical security is largely aimed at providing adequate safeguards for electronic protected health information (ePHI) as well as maintaining a state of readiness to access the information and run vital health care operations on a continuous (or near continuous) basis.

Physical security has long been recognized as a critical component of any comprehensive information security program. Accordingly, it is given substantial weight in the HIPAA Security Rule (see below). From small, rural physician practices to large, urban hospitals or insurers, good physical security is essential for protecting information and equipment.

Of the three major "pillars" for information security (technical and administrative security being the other two), physical security concepts are perhaps the simplest to grasp for the average person (that is, for those who are not IT security professionals). This is because we can relate many of the principles of physical security to everyday life. For example, the door and window locks on our homes represent a basic form of physical security that is equally valid for protecting computer equipment inside a data center. Alarm systems such as those that protect automobiles can also be used to deter or detect unauthorized intrusion into health care providers' facilities containing important computer systems and workstations. Conversely, there is widely publicized disregard for good physical security practices, such as in the case of laptop computers containing large volumes of ePHI that are left in automobiles or homes and consequently stolen.

Legal Requirements

While it has long been recognized as good business practice, physical security was codified into law for covered entities in section 164.310 of the HIPAA Security Rule. Section 164.310 groups physical safeguards into four primary categories: facility access controls, workstation use, workstation security, and device and media controls. Within two of those categories, there are additional subsections addressing requirements for contingency operations (eg, disaster recovery and business continuity), facility security plans, re-use and disposal of computer media (for example, magnetic types or CDs), and more. The major categories and some of the subsections are described further below.

[3] John C. McKenney, CIPP, SEC Associates, Inc.

Facility Access Controls

As the name implies, this section addresses expectations for controlling and protecting access to the physical building(s) that house electronic information systems, and access to those systems once inside the premises. The intent is that authorized persons should be permitted access (without unreasonable delays or barriers), while unauthorized persons should be prevented, or at least deterred, from gaining access (and that unauthorized access should be detected and reported in a timely manner). Typical examples of facility access controls include door and window locks, electronic access controls (eg, badge readers), alarms, security guards, and video surveillance systems. Additionally, access controls include not only the hardware components such as locks or alarms, but also the policies, procedures, and training regarding their proper use, reporting, maintenance, and so on.

Other considerations within this category of physical safeguards include contingency operations, facility security plans, access control and validation procedures, and maintenance records. Contingency operations refers to providing appropriate facility access controls in the event that emergency or disaster recovery operations are in effect and "normal" facility access controls may not be operational (for instance, business recovery operations may be running out of completely different facilities). The facility security plan defines and documents the safeguards deployed to protect the facility or facilities. Access control and validation procedures refer to mechanisms used to ensure the identity and role of each person entering the facility, and to control their access to electronic information systems once inside the facility. Maintenance records refers to the need for organizations to carefully document repairs and maintenance performed on facility access controls that impact facility security in any way.

In addition to lock or alarm system maintenance, this would include regular maintenance of fire suppression equipment and emergency exits. Providing security for staff while maintaining means of egress in the event of a disaster are both part of the contingency portion of physical security.

Workstation Use

Every organization that handles ePHI must have policies, procedures, and training that clearly define proper and improper uses of computer workstations with access to ePHI. In most cases, workstations can be thought of as laptop or desktop computers, and the electronic media associated with them, such as tape drives, flash drives, CD/DVD writers/ players, and so on. It is essential that workstation users have appropriate information and training about proper use to minimize the risks to such systems, including virus attacks or breach of confidential information.

Workstation Security

In addition to ensuring that users are properly trained on workstation use, it is also important to provide appropriate security controls for workstations that can access ePHI. There is a broad range of options that can be implemented depending on the circumstances. For example, it may be adequate to secure a workstation by keeping it in a locked room with limited, controlled access to the room. In other cases, such as a busy nurses' station in an open area, other types of controls may be required to restrict access to authorized users.

Device and Media Controls

An area of critical importance with regard to physical security is that of providing appropriate controls around digital devices and media that can contain large volumes of ePHI in a very small physical form. Digital memory cards (also called memory sticks, flash drives, and various other names) can contain gigabytes of data on devices smaller than a pack of chewing gum. Their small size makes these devices especially vulnerable to theft or loss, and they make it easy to move large amounts of data. CDs and magnetic tapes, while somewhat larger, are also subject to the same vulnerabilities. Organizations responsible for ePHI must have documented policies and procedures for appropriate use of, and controls around, any such devices and media. These procedures must include controls concerning the disposal and/or re-use of digital media; accountability for tracking the use and whereabouts of devices and media; and data backup and storage of ePHI before movement of equipment, to ensure that ePHI records can be retrieved in the event of a problem.

Summary

Principles of physical security have existed since long before computers and ePHI. Preventing or deterring intruders from entering secure facilities and ensuring that visitors are properly recorded and escorted are two examples of physical security that predate information technology. The fact that many forms of physical security are "ancient" when compared to the age of computer technology in no way diminishes the importance of this critical aspect of the overall IT security strategy. It is essential that every facility that houses ePHI have well-documented controls, policies, and procedures commensurate with the level of risk to the protected information. In addition, all persons with access to computer workstations and other assets must be trained on the policies and procedures governing the physical security controls. When combined with well-managed administrative and technical controls, physical safeguards play a critical role in helping to ensure the privacy, security and availability of ePHI.

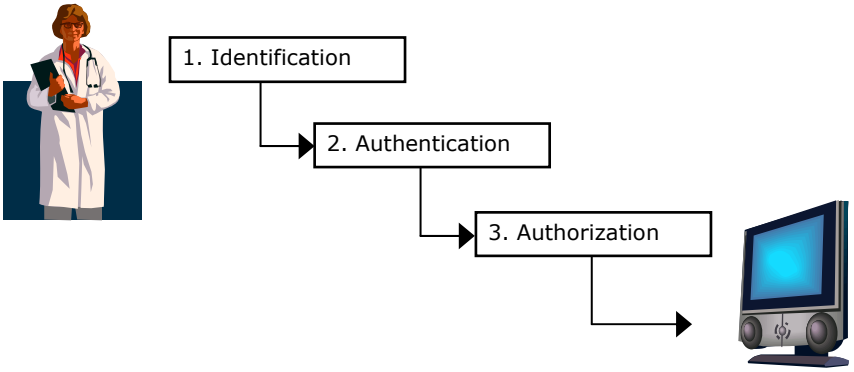
PART 4:
TECHNICAL SECURITY

D4.1: ACCESS CONTROLS[4]

Introduction

The term "access controls" describes a broad category of security mechanisms and policies designed to help ensure that computer and physical resources are used only for their intended and authorized purposes. Three primary components of access controls are: identification, authentication, and authorization. This section discusses access controls and authorization, and to a lesser extent, identification and authentication. Authentication is described in more detail in ***Part D4.4, Authentication***.

Access controls can apply at all levels. For health care systems, protections must be in place to control access to the network; to individual computers and devices on the network; and even to individual applications, or programs, on the computers as well as access to the physical facility. We typically think in terms of controlling the access of people to the system components, such as ensuring that only authorized users have access to protected health information (PHI). Access controls, however, also apply to computers, software, and facilities, to ensure that computers and software programs can only access other data and programs for which they have the proper "permissions." The purpose of access control is to ensure that only authorized members of the workforce, business associates, or authorized entities such as RHIOs have access to facilities housing computer systems and work areas where PHI s stored. For simplicity, the rest of this discussion is limited to access controls for human users. We will also exclude from this discussion the category known as "physical access controls" (for example, security guards and cameras, badge reader door locks, and so on). Access controls for access by other computers as well as physical security/access does need to be considered but will not be covered in this section. The diagram below helps illustrate the relationships between three critical elements of computer access controls.



Access Controls

[4] John McKenney, CIPP, SEC Associates, Inc.

Identification, Authentication, and Authorization

Consider a simple example of a physician who needs to access a patient's medical records online. First, Dr. Smith must identify herself to the computer system. Identification is typically performed by entering a user name, which may consist of first initial and last name, perhaps with some numbers added to make the user name unique. However, since the user name may be (and often is) publicly available, anyone could type in Dr. Smith's user name to try to "fool" the computer. The second access control step—authentication—is implemented to try to prevent fraudulent impersonations of this type. In simple terms, to authenticate is to "convince" the computer that you are who you say you are by providing evidence to support your claim. The most common way of doing this is to type in a password that should be known (in this case) only by Dr. Smith. Since no one else should know Dr. Smith's password, she has now authenticated her identity to the computer. This is also called single factor authentication.

As a side note, authentication can be broken down into three areas: what you know (your password), what you have (a smart card, a security token, etc.) and who you are (fingerprint readers, retinal scans, etc.). Most organizations rely on single factor authentication (a password). Depending on the sensitivity of the data stored, organizations may need to consider multiple factor authentication such as using a password in combination with a smart card.

At this point, Dr. Smith has merely entered the "front door" of the computer system. There is processing going on "behind the scenes" to determine just which applications and data on the computer system Dr. Smith has permission to access. This is the third access control step, known as authorization. In a properly configured system, Dr. Smith will only be authorized to access programs and records on the system to which she is entitled by law and by other rules put in place by the organizations she works with and for. For example, if Dr. Smith sees patients at a hospital where she is not on the hospital staff, she may only be authorized to access the records of her patients, whereas hospital staff doctors may have access to the records of all patients in the hospital. This is an example of the concept of "least privilege," which means that users' access to applications and records on the system should be limited to the smallest subset which they need to perform their duties efficiently. In this example, Dr. Smith has no reason to access the records of other hospital patients who are not her patients, and she therefore should not be granted access to those records.

A close "cousin" to "least privilege" is the authorization concept referred to as "need to know." Continuing the example with Dr. Smith, the hospital's financial accounting software may be accessible from the same terminal where she is accessing her patient records. However, since she has no need to know anything about the hospital's financial records, her authorization profile should prevent her from accessing the accounting software. Ideally, the authorization profiles for all users should be based on the concepts of "least privilege" and

"need to know." In reality, employees often move around in an organization, and as they move to new positions and are given new authorizations to match their duties, some of their old authorizations should be removed or deactivated. This is why it is important in any organization to periodically review the authorizations for every employee (and for consultants and contractors) to be sure that the principles of "least privilege" and "need to know" are in force and current.

Legal Requirements

Section 164.312(a)(1) of the HIPAA Security Rule requires covered entities to implement access controls to electronic information systems as a means of safeguarding electronic protected health information (ePHI). The expected access controls include technical policies and procedures that are intended to "allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4)." In addition, some states may have more stringent or prescriptive access control requirements.

Granting Access Rights

As described above, authorization is the access control step that determines what resources within a computer or network that any given user can access. This capability is achieved through the process of granting access rights before the user can get to those resources. Access rights can be established in many different ways and at various levels, only a few of which will be described here.

Access rights can range from complete, unrestricted access, to no access whatsoever, and everything in between. Many home computers are configured for unrestricted access, meaning that any family member (or any other user, for that matter) has full access to any and all programs or data on the computer. For entities that handle ePHI, however, unrestricted access for all employees is not an acceptable option. One option would be to configure access rights for each individual user of the system. While this option provides the most flexibility, with the ability to create a customized access profile for every user, it is also creates substantial maintenance overhead.

A better approach is to implement role-based authorization or role-based access control, whereby the same set of access rights is automatically configured for each user associated with a particular role. Examples of roles that could be defined are emergency room nurse, radiologist, or claims processor. The access rights for all radiologists would be the same, but those access rights might differ from the access rights for all ER nurses. A third method of controlling access rights is known as group-based access control, in which all users in the same group or area are issued common access rights. One group might be all lab personnel (regardless of specific role); another might be all ER staff (again, without regard for role). While group-based authorization has some of the efficiency benefits of role-based authorization, it is less desirable because it does not necessarily enforce "least privilege"

and "need to know" principles within a group. Generally speaking, role-based access control needs to allow for exceptions that may be necessitated by special projects, or when a member of the workforce is covering for an absent employee. Role-based access also must fit the needs of the organization. If it is too complex, it is difficult to administer. If it is too simple, it creates a situation where individuals may gain access to systems and data for which they are not authorized.

As mentioned earlier, access rights can be implemented at various levels—from the network operating system, to the computer operating system, right down to the individual application software and external media that may be used with a particular workstation. The process of deploying and maintaining access controls across many different computer platforms and applications can be quite complex and time consuming. In addition, users have difficulty remembering the various identifiers (eg, user names) and authentication codes (eg, passwords) for the multitude of systems and applications that they use in their work. Consequently, there is growing interest in a class of solutions known as "single sign on," or SSO.

Single Sign On

Without getting into the details and variations of SSO solutions, the central idea is that a user needs only a single identifier/authentication pair, and the SSO software will manage authenticating that user on every system, computer, and application for which that user has been authorized. For the user, the main benefit of SSO is not having to remember (and type in) a plethora of user names and passwords for all the applications they need to access. The primary risk of SSO is that if a user's SSO user name/password are acquired by a hacker or another member of the workforce with the intent to damage the organization, that hacker or workforce member now has access to all of the systems and applications to which the rightful owner has access. As a result, secure SSO implementations that make use of two-factor, or strong authentication techniques, are highly recommended, as discussed in ***Part D4.4, Authentication***.

Access Control Product Vendors

The concepts discussed in this section—identification, authentication, and authorization—are all components of access controls. As discussed above, some or all of these components can be found in many software applications, and in virtually all operating system software. However, to provide better, more consistent security controls, with better management and maintenance capabilities, many vendors offer products to manage access controls across a variety of applications and platforms. These products may be referred to as Identity Management systems, and may offer additional security features, such as audit trails.

Following is a list of vendors that supply products that include authorization and access controls. RTI International does not endorse any of these vendors and has not tested these

products. This list is not all-inclusive, but provides a starting point for an organization, stakeholder group, or subcontractor to locate potential vendors.

- Computer Associates (http://www.ca.com)
- Entegrity Solutions (http://www.entegrity.com/)
- Entrust (http://www.entrust.com/)
- Hewlett-Packard (http://h20229.www2.hp.com/products/select/index.html)
- IBM (http://www-306.ibm.com/software/tivoli/products/federated-identity-mgr/)
- Novell (http://www.novell.com/products/ichain/samlextension/quicklook.html)
- Oracle (http://www.oracle.com/products/middleware/identity-management/identity-management.html)
- RSA Security (http://www.rsa.com/)
- Secure Computing (http://www.securecomputing.com/)
- Spyrus (http://www.spyrus.com/)
- Sun Microsystems (http://developers.sun.com/prodtech/javatools/jsenterprise/index.jsp)
- Timberline Technologies (http://www.timberlinetechnologies.com/)
- Vasco (http://www.vasco.com/)
- VeriSign (http://www.verisign.com/)

Summary

The term "access controls" defines a broad category of security mechanisms, techniques, and procedures that are designed to ensure that only authorized users and programs can use the resources of restricted computers, programs, and data. Identification, authentication, and authorization are key components of technical access controls. The first two require the user to answer the questions: "Who are you?" and "Why should I believe you?" When the first two are satisfied, authorization says: "Now that I know who you are, here is what you have access to." These three access controls, when properly implemented with appropriate procedures and training, can provide a secure information system environment that adequately safeguards ePHI.

D4.2: ANTIVIRUS & ANTISPYWARE SOFTWARE[5]

Introduction

The purpose of this part of the IT Privacy and Security Primer is to describe what antivirus software and anti-spyware software are and why it is important to deploy them. Today all organizations that access the Internet receive e-mail with attachments or download files from an outside source risk network or computer infection by a virus, Trojan, or worm that could shut down a network or a computer and/or infect other computers on the network. Spyware is another security risk that needs to be addressed. Generally downloaded when an Internet site is accessed, spyware can track what web pages are visited and send information such as passwords or keystrokes to a third party. Antivirus and anti-spyware software protects organizations from such threats. Antivirus software is also specifically referenced in the HIPAA Security Rule as an addressable item (45 C.F.R. pt. 164.308(a)(5)).

Antivirus Software

Antivirus software can detect and stop the infection of networks and computers by viruses, trojans, and worms, but only if properly used. There are a number of software applications on the market that fall in the category of antivirus software, and applications range from single computer use to network use. It is a sound practice to purchase antivirus software, load it on organizations' networks, and, in the case of small offices, individual computers.

The software, though, is only effective if it is regularly updated, if virus scans are regularly performed on the computers, and if the workforce is properly trained on its use. It is also sound practice in larger organizations to employ more than one antivirus software application because if one application misses a virus, trojan, or worm, the other application is likely to catch it and keep it from infecting a computer system.

Antivirus software operates from what are called signature files. These files are continuously updated by application vendors and assist organizations in keeping a current record of new viruses, trojans, or worms that are let loose on the Internet. A signature file needs to be updated at least weekly (more frequently if the organization so chooses) so the organization has a record of all present and new viruses, trojans, and worms that could infect a network or computer. It is generally the responsibility of the information technology (IT) staff to update signature files except in small organizations where this duty may fall to individual members of the workforce.

It is also important to periodically run scans of networks and computers to make sure no viruses, worms, or trojans have been introduced into an organization's technical environment. This requires using the scan function of the application, during which the software scans all the files, the operating system, and other related applications to

[5] Chris Apgar, CISSP, Apgar and Associates, LLC.

determine if any viruses, worms, or trojans have infected the system. The application also assists in "cleaning" the system if a virus, Trojan, or worm has been discovered.

Equally important is workforce education. It is wise to implement policies that prevent workforce members from loading any software that has not been scanned and has not been approved by the organization for deployment. This includes software brought from home and software downloaded from the Internet.

Another source of viruses, worms, and trojans is e-mail. As part of workforce education, it is a good idea to require that workforce members not open any attachments with an .exe extension or other program extension. Also, it is a good idea to inform workforce members that if they receive an attachment from someone unknown to them or one that looks suspicious, even if sent from a trusted individual, to contact the individual who sent the attachment before opening the attachment and also to scan the attachment before opening it.

Internet messaging (IM) or "chatting" is becoming more and more common for personal and business needs. It is generally available for free through certain websites. Besides representing a danger to the privacy of information communicated during chat sessions, IM represents a significant vulnerability when it comes to viruses, trojans, and worms. These can be transmitted from one computer to another just by signing on to a chat session. Some organizations have banned IM because of this threat and the threat to the privacy of the data. Organizations that allow IM need to be aware of the associated risks.

Following is a list of antivirus software vendors. RTI International does not endorse any of these vendors and has not tested these products. It is not complete but provides the reader a place to start when evaluating antivirus software applications they may wish to purchase and install in their environment.

- Bitdefender—http://www.bitdefender.com/site/Products/showSolutions/3/
- NOD32—http://www.eset.com/landing_pages/landing_page1.php?threat=antivirus&gclid=CI3t8rOfi4sCFRgZYAodgkI9Gw
- Kaspersky—http://www.kaspersky.com/personal?AID=10273799&PID=1717916
- McAfee—http://www.mcafee.com
- netiQ—http://www.netiq.com/products/smp/xmp_ava.asp
- Panda Antivirus—http://www.pandasoftware.com/?track=31135&idioma=EN&pais=63
- Symantec/Norton—http://shop.symantecstore.com/store/symnahho/en_US/DisplayHomePage/pgm.5937500/ThemeID.106300
- The Shield—http://www.pcsecurityshield.com/webApp/90042.asp?trk=DTK&bid=29&aid=CD567&opt=Goog-antivirus+software
- Trend PC-cillin—http://www.digitalriver.com

Antispyware Software

Most spyware can be downloaded to a network or a computer without the user knowing it. Generally spyware comes in the form of what is called a cookie. There are two types of cookies. One that is called "session only" that helps properly display the web page and is not used after the user leaves that particular website. The other is downloaded and is stored on computers or networks and is often used to track web surfing patterns. It can also be used to download spyware that can detect passwords, track e-mail, and read key strokes. In the latter case of malicious spyware, after it records keystrokes that may include passwords and other proprietary information, it can automatically upload those data to a host computer on the Internet, all without the knowledge of the user whose computer was compromised.

A number of organizations have elected to not allow cookies to be downloaded when a workforce member visits a website. This does provide protection against downloading unwanted spyware but can get in the way of website operation. Cookies are used by a number of websites to properly display material and some websites will not allow access if cookies are not allowed. This becomes a business decision of the organization—the balancing of security risk with business needs.

There is software available on the market that detects spyware not only in cookies but spyware that may be stored as a mini-application on a network or computer in the operating system registry. It is a good idea to purchase antispyware and, just like antivirus software, it needs to be updated regularly, run regularly, and staff need to be trained on its use.

Antispyware, if used correctly, is used to scan computers or networks to detect spyware or suspected spyware. The user is given the option of deleting the spyware or potential spyware and the antispyware software "cleans' the computer or network. The key is that the application needs to be regularly updated (just like antivirus software, antispyware software relies on signature files) and regularly run.

This is especially critical given the nature of malicious spyware. It is a good idea for organizations to protect against malicious software that tracks Internet activity, can detect passwords, track e-mail, and track key strokes, especially if the organization uses the Internet frequently and transmits confidential or proprietary data.

Following is a list of antispyware software vendors. RTI International does not endorse any of these vendors and has not tested these products. It is not complete but provides the reader a place to start when evaluating antispyware software applications they may wish to purchase and install in their environment.

- Ad-Aware—http://www.lavasoft.de/
- Giant Antispyware—http://www.softpedia.com/get/Internet/Popup-Ad-Spyware-Blockers/GIANT-AntiSpyware.shtml

- Microsoft Windows Defender (beta)—http://www.microsoft.com/athome/security/spyware/software/default.mspx
- PestPatrol—http://www.ca.com/products/pestpatrol/
- Steganos—http://www.steganos.com/?product=saspy2006&language=en
- McAfee—http://www.mcafee.com
- Spyware Doctor—http://www.pctools.com/spyware-doctor/?ref=g77
- SpySubtract—http://www.intermute.com/products/spysubtract.html
- Spy Sweeper—http://www.webroot.com/land/freescan_ent.php?rc=3837&ac=807&wt.srch=1&wt.mc_id=807
- Symantec/Norton—http://shop.symantecstore.com/store/symnahho/en_US/DisplayHomePage/pgm.5937500/ThemeID.106300

Summary

It is sound security practice to install antivirus and antispyware software on organization computers and networks. The cost is generally fairly low and the protection both applications provide is significant. Keep in mind that addressable does not mean optional. It means an organization must adopt the implementation specification as defined in the rule, adopt an alternative that is equivalent or provide sufficient documentation why the implementation specification is not required (and it cannot be solely due to cost). Given the affordability of reliable antivirus and anti-spyware applications, an organization would be hard pressed to justify not installing them.

D4.3: AUDIT LOGS AND AUDIT PROGRAMS[6]

Introduction

The purpose of this part of the IT Privacy and Security Primer is to describe what audit logs are, appropriate practices for audit log use, and the appropriate practice of establishing a formal security and privacy audit program. Audit logs are an important method of tracking activity on a computer system as well as tracking what members of the workforce or others with access to your system do, especially while accessing sensitive data.

Many applications and network operating systems generate audit logs. The purpose of an audit log is to allow the auditor or person assigned with the task of monitoring system or application activity a method of capturing the information related to activity on the network, user-made file changes, user-made file additions, user viewing confidential data, etc. Without audit logs it is difficult to adhere to the HIPAA Security Rule requirements that relate to audit controls and information system activity monitoring.

One of the problems organizations face is that some software applications either do not include needed audit logs, do not include enough audit logs, or do not include any audit logs. This is primarily a problem with what are called legacy systems. Legacy systems are older applications that are often no longer supported by the vendor. Many legacy systems do not include audit logs so organizations are often forced to develop manual methods such as comparing input forms with the electronic record to audit legacy systems.

One of the key things to remember about audit logs is that organizations need to fully define what they intend to audit, establish an audit schedule, and above all ensure that any audit logs retained are actually looked at. If all audit logs are turned on, generally two things happen: (1) organizations find themselves buried in paper or electronic files that, from a staffing point of view, would be impossible to look at; and (2) it creates a liability for the organization. If an organization collects audit data but does not look at it, a civil liability is created in the event that patient information is inappropriately released and the patient wishes to file suit. The claim would be, "you had the information but you did not look at it." This is why it is important to complete some initial planning before deciding which audit logs to turn on.

The basic guideline to follow is that if you do not intend to review the audit log that would be generated, do not turn it on. This does not mean, though, that all audit logs should be turned off. It is important to monitor certain critical activity to meet appropriate security standards, protect the organization, and comply with the HIPAA Security Rule.

It is important for organizations to develop a formal audit program that makes use of the audit logs that are maintained. An audit program needs to be formal, organized, collect data

[6] Chris Apgar, CISSP, Apgar and Associates, LLC.

on critical areas of operation in an organization, and should be conducted on a regular basis. The purpose of an audit program, besides compliance with HIPAA, is to assess system activity to determine if threats and vulnerabilities crop up, data are inappropriately used and then to change policies and procedures where necessary to reduce the risk to the organization.

Most audit programs are initially based on the HIPAA required risk analysis. During a risk analysis, an organization determines assets (data, hardware, software, people, etc.), evaluates any threats or vulnerabilities to those assets, evaluates current safeguards, assesses the likelihood of an adverse event occurring and determining the cost to the organization. After the risk analysis, the organization moves into the risk management phase (also required by HIPAA). The purpose of a risk management program is to reduce the likelihood a threat or vulnerability will be exploited. Part of that process is developing an appropriate audit program.

After determining what is critical to the organization and identifying existing threats and vulnerabilities, it is far easier to develop a thorough audit program. As part of the audit program development process the number and types of audit logs are evaluated and a determination is made as to whether certain event logging (audit logs) will assist in protecting critical assets of an organization and assess identified threats and vulnerabilities (ie, whether an adverse occurrence has been discovered, if threats and vulnerabilities are adequately addressed, and so forth).

After available audit logs have been assessed and it is determined which audit logs would be appropriate to support an organization's audit program, the next step is to turn on identified audit logs. The audit logs should be maintained in a central location if feasible so they are available when the actual audit is conducted.

There may be times when audit logs need to be reviewed on a more regular basis. As an example, the HIPAA Security Rule requires information systems monitoring. That activity will likely require a more frequent review of system-generated or network audit logs such as firewall logs, intrusion detection logs, and antivirus logs. Organizations may also elect to conduct random audits of access to the electronic health record, for example, to determine if the record has been inappropriately accessed or modified. This is a determination that is up to each organization and will likely depend on individual business practices as well as business policy.

Audit programs are not static. Organizations should periodically review what is being audited to determine if the criteria continue to meet the requirements related to monitoring critical functions and identified threats and vulnerabilities. This also means a risk analysis should be conducted on a regular basis to assist in maintaining current and appropriate audit criteria. It is recommended that audits and risk analyses be conducted at least annually or when any major change occurs to the business or technical infrastructure.

It is also important to remember that audit findings need to be addressed. An organization may determine that no further action is necessary on a finding because it has little effect on the organization; the determination and finding need to be documented. Also, if an audit report identifies needed changes in policies, procedures, practices, implementation of a training program, the acquisition of new software, or changes in the technical infrastructure, the organization needs to take positive action to either address what is identified in the audit report or document why no action will be taken. A liability is created if an organization chooses not to address any audit findings. If an identified action is not taken and the organization knows about it but has not documented the reasons for not acting, the organization is vulnerable to civil action. Also, under the new HIPAA Enforcement Rule, this could be viewed from a regulatory perspective as "willful neglect," which leads to a higher likelihood that OCR or CMS may elect to pursue civil penalties under HIPAA rather than informally work with the organization to address any noted violations. The organization has in essence not demonstrated due diligence.

Software

There are a number of resources on the market and available for free that can assist organizations in developing an appropriate audit program to meet regulatory requirements and business needs. It is important when creating an audit program to make sure that the audit program meets the needs of the business instead of just the regulatory requirements. As an example, an organization may determine that a frequent and more stringent audit program is most appropriate for its business even though it might not be required by the HIPAA Security Rule.

Some of the resources available to assist organizations develop an effective audit program and appropriately use audit logs follows. This list is not all inclusive and none of the vendors or organizations are endorsed by RTI International.

- AIS (HIPAA Patient Privacy Compliance Guide)—http://www.aishealth.com/AISCompliance.html
- AKT—http://www.aktcpa.com
- HCPro—http://www.hcpro.com
- HIMSS—http://www.himss.org/ASP/index.asp
- ISACA—http://www.isaca.org
- MIS Training Institute—http://www.misti.com
- NIST (800 Series)—http://www.nist.gov
- WEDI—http://www.wedi.org

Additional information may be available through associations to which organizations belong. There is the option of outsourcing at least initial construction of an audit program. It is advisable when outsourcing to contact reputable consulting firms, require potential

candidates to be certified (Certified Information Systems Auditor or CISA) and require that potential candidates know the business of the organization—to know health care and associated regulations.

Outsourcing has the advantage of assisting organizations to create a robust audit program that addresses privacy and security. It also assists the organization to "create" an audit program that can be conducted by internal staff after implementation. This does not mean audit programs are static. It only means the audit program can grow and change with the organization based on a sound audit program design.

D4.4: AUTHENTICATION[7]

Introduction

Person or entity authentication is the process of establishing that a particular user (or entity) is who they claim to be. For purposes of this discussion, it can be assumed that "person" and "entity" are synonymous and interchangeable.

The HIPAA Security Rule requires that before a person is granted access to ePHI, the following questions must be answered: "Who are you?" and "Can you prove it?" The first question deals with *identification*, whereas the second deals with *authentication*. Identification is the act of stating who you are, often by presenting a username or e-mail address (note: the HIPAA Security Rule requires that users have unique user names). However, since these identifiers are often publicly accessible, it would be easy for someone to impersonate you if identification was all that was required to gain access to ePHI. Authentication is the process of demonstrating that you are indeed who you say you are. This is typically achieved by providing one or more of the following additional, private pieces of information which are often referred to as something you know, something you have, or something you are, as explained below.

The most common form of authentication is the use of a password (something you know) that is supplied with the identification (such as username). Other forms of authentication include something you have (for example, an ID badge, smart card, or token) and something you are (for example, a voice print, finger print, or retinal scan). "Two-factor authentication," also called "strong authentication," is the process of using two independent forms of authentication to establish a strong link to one's identity. A familiar example is that of a bank ATM, where two-factor authentication is achieved with a bank card (something you have) combined with a personal identification number, or PIN (something you know). In the ATM example, an impersonator would need not only the bank card, but also the PIN; one or the other alone would not give the impersonator access to the money. Contrary to a popular misconception, the combination of a unique user ID and password does not represent two-factor authentication, because the user ID is often publicly available.

The basic purpose of authentication is to provide a degree of assurance (scaled appropriately to the potential consequences of unauthorized access) that the user or entity truly is who they claim to be.

Legal Requirements

Section 164.312(d) of the HIPAA Security Rule requires covered entities to "Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed." This means that covered entities must take steps to

[7] John C. McKenney, CIPP, SEC Associates, Inc.

safeguard their ePHI with appropriate authentication controls and procedures. As mentioned above, authentication controls can take a variety of forms. They usually include a combination of administrative and technical measures that are based on a risk analysis to achieve the appropriate level of protection. Note too that the HIPAA Privacy Rule requires authentication when accessing PHI. Some of the available authentication options are discussed below.

Types of Authentication

Many types of authentication are in use today. The effectiveness, cost, ease of use, and human acceptability of these approaches varies widely. A few of the most common authentication mechanisms include passwords, PINs, tokens, and biometrics. Strengths and weaknesses of these authentication methods are discussed below.

Passwords—Reusable passwords are the simplest, least expensive, and most common form of electronic authentication in use today. Nearly every person who has used a computer is familiar with entering their username followed by their password. Most operating systems and applications provide at least some level of password authentication. However, while passwords may be the most common and least expensive mechanism for authentication, they are also considered by security professionals to be one of the weakest forms of security.

There are many reasons that passwords typically are a weak link in the security chain. Some of these reasons include: passwords are often created by the user, and can be easily guessed (such as a spouse or pet name, birth date, or phone number); passwords can be easily shared with others; passwords can be captured by keyboard logging software or hardware, and can even be observed by watching a user type their password; passwords can be "sniffed," or intercepted, over a network connection, if the password is sent unencrypted; trusting users can even be coaxed into revealing their passwords to criminals posing as IT support specialists. Passwords have many more vulnerabilities, but these are a few of the most common. Since passwords remain the most used form of authentication, it is very important to implement and manage strong password controls in order to minimize the risk.

Personal Identification Number (PIN)—PINs are a type of password, and thus have the same weaknesses as the password types discussed above. They are listed separately here only because they have been in common use for so many years (usually associated with bank ATMs) that some readers might not think of them as passwords. PINs are, however, often distinct from typical passwords in two respects. For one, they frequently consist of only 4-digit numbers, making them relatively easy to "crack" with the right software tools. For another, users tend to not change their PINs unless there is a compelling reason to do so (such as loss of their ATM card), which makes them vulnerable if the PIN should be

compromised without the owner's knowledge. For both of these reasons, PINs alone should not be used for authentication, but PINs can be effectively used in combination with another authentication mechanism (such as a bank card or token).

Tokens—Also called security tokens or hardware tokens, tokens represent a class of small devices that can be issued to computer users for use during the authentication step. The token stores special authentication information that the user might key into the computer. Alternatively, many tokens plug into the computer and supply the information directly through the connection. Tokens are small and easily carried in a user's pocket or on a key chain. When used in combination with a PIN (see above), tokens provide strong authentication. The main drawbacks to tokens include relatively high cost (some of the systems are proprietary, thus affecting pricing), token management, and the possibility that tokens can be shared, lost, or stolen.

Biometrics—This refers to a method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable.[8] There are many types of biometric identification schemes. Examples include measurement of the:

- **face:** the analysis of facial characteristics,
- **fingerprint:** the analysis of an individual's unique fingerprints,
- **hand geometry:** the analysis of the shape of the hand and the length of the fingers,
- **retina:** the analysis of the capillary vessels located at the back of the eye,
- **iris:** the analysis of the colored ring that surrounds the eye's pupil,
- **signature:** the analysis of the way a person signs his or her name,
- **vein:** the analysis of pattern of veins in the back of the hand and the wrist, and
- **voice:** the analysis of the tone, pitch, cadence and frequency of a person's voice.

Biometrics offer several important advantages for authentication. For example, they are unique; they cannot be "shared" with another person like a password or ID badge can; they are not easily faked or copied for fraudulent purposes; and they do not have to be remembered. On the other hand, there are many drawbacks to biometrics, which explains why they have not enjoyed greater acceptance to date. Some of these drawbacks include: concerns about privacy and/or intrusiveness; ineffectiveness of some of the methods in environments requiring gloves, eye shields, or head coverings; false positives and false negatives; and cost.

[8] 21 C.F.R. pt. 11: Electronic Records; Electronic Signatures; Final Rule. Food and Drug Administration, Dept. of Health and Human Services, March 20, 1997.

Authentication Product Vendors

Following is a list of vendors that supply authentication products. Note that authentication is frequently bundled within a more comprehensive product offering several other functions such as identification, authorization, and more. These products may be referred to as Identity Management systems. RTI International does not endorse any of these vendors and has not tested these products. This list is not all-inclusive, but provides a starting point for an organization, stakeholder group, or subcontractor to locate potential vendors.

- Computer Associates (http://www.ca.com/) *
- Entegrity Solutions (http://www.entegrity.com/) *
- Entrust (http://www.entrust.com/) *
- Hewlett-Packard (http://h20229.www2.hp.com/products/select/index.html) *
- IBM (http://www-306.ibm.com/software/tivoli/products/federated-identity-mgr/) *
- Novell (http://www.novell.com/products/ichain/samlextension/quicklook.html) *
- Oracle (http://www.oracle.com/products/middleware/identity-management/identity-management.html) *
- RSA Security (http://www.rsa.com/) *
- Secure Computing (http://www.securecomputing.com/)
- Spyrus (http://www.spyrus.com/)
- Sun Microsystems (http://developers.sun.com/jsenterprise/index.jsp) *
- Timberline Technologies (http://www.timberlinetechnologies.com/)
- Vasco (http://www.vasco.com/)
- Verisign (http://www.verisign.com/)

* Indicates companies that have products listed in the "Approved E-Authentication Technology Provider List" on the federal CIO website (http://www.cio.gov/eauthentication/documents/ApprovedProviders.htm). Note that the products were approved for a specific Federal agency E-Authentication Initiative, and may or may not be suitable for any particular health care stakeholder organization.

Summary

Authentication is a critically important step in the process of ensuring that unauthorized persons or entities are prevented from accessing ePHI. Good authentication mechanisms should not be unduly burdensome, slow, or costly if they are to be feasible across the broad community spectrum of health care stakeholders. Although a password combined with a username continues to be the most common form of authentication, health care entities need to consider stronger controls and authentication mechanisms in order to ensure both the protection of patient information and compliance with HIPAA.

D4.5: ENCRYPTION[9]

Introduction

Encryption is a form of securing the transmission of confidential or proprietary information or data at rest. It is based on a mathematical formula and comes in many forms from secure e-mail to virtual private networks to encrypting laptop hard drives. Encryption is referenced in the HIPAA Security Rule (45 C.F.R. 164.312(a)(1) and 45 C.F.R. 164.312(e)(1).

There are many forms of encryption suitable for different needs of an organization. The purpose of this section is to provide information about the use of encryption to secure confidential and proprietary information in transit and at rest. It is not meant to provide states with a definitive standard because each state and each organization within a state will have varying needs as it relates to securing data in transit and at rest.

Legal Requirements

The HIPAA Security Rule references encryption for protecting data in transit and at rest. It is included as an implementation specification and is addressable. This does not mean it is optional. What addressable means is that a covered entity under HIPAA has three choices—implement encryption technology, implement an alternative technology that is equivalent to encryption, or soundly document why the implementation specification will not be implemented.

Given the number of encryption options and the availability of encryption technology for small to large organizations, it would be difficult to justify not implementing encryption to protect data in transit and data at rest. This section will describe different methods of encryption and include a list of alternative vendors offering encryption technology.

What Encryption is Not

Encryption is not a method of authenticating a user of the data to determine if the individual or entity has a right to view the data. It is also not a method of authorizing access to different levels of data. Encryption is a technology that protects data in transit or at rest in the event transmitted data are intercepted or for example when a laptop with confidential information is stolen or lost.

Encryption protects data from being read by unauthorized individuals who intercept it. It is a method of protecting data at rest from being viewed by an unauthorized user. It is also a method of preventing corruption or manipulation of intercepted data by unauthorized users.

[9] Chris Apgar, CISSP, Apgar and Associates, LLC.

Types of Encryption

There are a number of different types of encryption. One thing to keep in mind when evaluating encryption solutions is the level of encryption (ie, 128 bit, 256 bit, etc.). The higher the level of encryption (the bigger the number), the harder it is for the encrypted data to be "cracked" or the mathematical formula protecting the data to be broken.

Types of encryption range from password protected encrypted files to what is called Public Key Infrastructure (PKI) to web messaging and others. Each type serves a purpose and defines a price range that an organization can use to evaluate whether or not a solution is viable for their organization. Types of encryption include:

Password-Protected Encrypted Files—This is generally the least expensive method of encrypting data when transmitting data over the Internet. The drawback to password-protected encrypted files is it requires the sender to share the password to the file with the recipient and often either requires the recipient to purchase the software or does not allow the recipient to respond in a secure fashion.

Password-protected encrypted files should not be confused with password-protected Excel spreadsheets or password-protected Word documents. These documents or files are not encrypted and are relatively easy to crack. Also, compressed files without encryption are not considered encrypted files and are also easy to crack.

PKI—Public key infrastructure, or PKI, is a method of encrypting data to be transmitted where the sender shares his or her "public key" with the recipient and the sender uses his or her "private key" to encrypt the message. To work, this requires an exchange of keys so messages can be exchanged in an encrypted format and the sender and recipient need to maintain what is called a key ring with all of the keys used by other organizations using PKI to encrypt and decrypt data.

The drawback of PKI is the complexity of large-scale rollout. There have been no large-scale rollouts of PKI to date. PKI can also be administratively burdensome to maintain. PKI is effective, though, if small numbers of entities or users are exchanging data such as when large volumes of data are exchanged between a few organizations such as clearinghouses.

Secure Web-based Messaging—This is one of the more common forms of encryption technology that has been deployed. It entails installing software or hardware on a network or employing an ASP that allows senders to transmit data securely by means of a website. The recipient receives a link to a website, opens the secure web page, and may be required to log on or provide appropriate authentication. The recipient is then able to access the secure data (including attachments) and respond securely to the message (including returning attachments). Web-based messaging is scalable and is reasonably priced for small organizations. It also is available in more robust forms for larger organizations.

Frequently web-based messaging is coupled with lexicon capabilities. In other words, functionality is made available that scans message content to determine if the message needs to be encrypted. The problem with lexicons is that they often provide too many false positives and encrypt data that do not need to be encrypted. A false positive is far safer than a false negative, which would allow messages that need to be encrypted to be sent via the Internet.

Secure Websites—More and more organizations are making confidential information available to patients and health plan members via company websites. Through the use of what is called secure sockets layer (SSL), information transmitted between the end user and the website can be secured. This is commonly used to view bank statements, credit card statements, and order goods online. This requires deployment of a secure web server and appropriate software. There are ASP options available on the market for smaller organizations that do not have the infrastructure to support a more robust and secure website.

Secure File Transfer Protocol (FTP)—Secure FTP is often used to transmit large files between entities. It bulk encrypts large files for transmission and allows for the transmission of, say, HIPAA-covered transactions. Often secure FTP is coupled with PKI because transmission is generally between a limited number of organizations.

Virtual Private Network (VPN)—VPNs can be likened to secure tunnels that span the Internet between organizations or between an organization and an employee who is a remote user of the organization's network. VPNs require the installation of hardware and software. VPNs are most frequently used by organizations that have remote users or telecommuters who regularly send and receive data that need to be secured between the remote user and the organization.

Secure Wireless—More and more organizations are moving to wireless networks. A good example is in hospital emergency rooms where laptops and handheld devices are used to collect information about a patient and wirelessly communicate with the hospital's network. Wireless networks require installation of hardware both on the network and on remote devices such as laptops to communicate with the wireless server. Wireless encryption software is available to secure any data transmitted between the laptop and the wireless server on the organization's network.

Hard Drive Encryption—There are several software applications on the market that allow a user or entity to encrypt hard drives (this even includes what is called flash memory on hand-held computers). Such software is important to consider if an organization uses laptops and hand-held computers because both are easily lost or stolen. Such software is generally inexpensive and secures the data stored on the hard drive or in flash memory. Such applications can also be used on servers used to store databases and large data files if the organization is concerned about unauthorized access to confidential or proprietary data.

Procedures for use of these applications must include password management to ensure that there is no loss of access to encrypted data due to personnel changes, forgotten passwords, and so on.

Folder Encryption—Instead of encrypting an entire hard drive, it may be preferable to encrypt at the folder level. Currently, Microsoft Windows XP Professional and Windows Vista Business or Ultimate allow encryption at the folder level, a functionality built into the operating system.

Encryption Vendors

Following is a list of encryption vendors. RTI International does not endorse any of these vendors and has not tested these products. This list is not all inclusive but it provides a place to start if an organization, stakeholder group, or subcontractor is in search of potentially suitable vendors.

- Certified Mail (http://certifiedmail.com)
- Cypherix (http://www.cypherix.com/cryptainerle/index.htm?source=adwords&keyword=encryption)
- Harris (http://www.harris.com)
- HushMail (http://www.hushmail.com)
- PGP (http://www.pgp.com)
- PriceGrabber (http://www.pricegrabber.com/)
- RSA (http://www.rsa.com/)
- Sigaba (http://www.sigaba.com)
- Tumbleweed (http://www.tumbleweed.com)
- VeriSign (http://www.verisign.com/)
- WinZip (http://winzip.com)
- ZipLip (http://www.ziplip.com)
- Zixcorp (http://www.zixcorp.com/)

Again, this list is not all inclusive and each vendor offers slightly different solutions that serve different sizes of organizations.

Challenges

No matter how reasonable, there is a cost associated with implementing encryption. Costs may include hardware, software, user training, policy development, and communication with partner organizations. Rate of return (ROR) or return on investment (ROI) may need to be calculated to persuade the organization and/or stakeholder group to make this investment. The thing to remember is that encryption is referenced in HIPAA and is considered sound security practice.

Rather than looking for ROI, a more productive perspective may be to view encryption as an insurance policy. Just as liability insurance provides organizations with protection against damage, encryption provides insurance against inappropriate interception, alteration, or access of confidential data or ePHI.

Another challenge to organizations is selecting the particular solution that suits the business needs of the organization and the budget. What works for a large health plan will likely not work for a small provider office. The above list of vendors provides a variety of options that will serve the needs of small to large organizations. To select the appropriate package, the organization will need to determine what is appropriate to serve the business needs of the organization and, especially with larger organizations, is robust enough to support additional users. This is especially important when considering the health care industry's move toward more consumer involved health care.

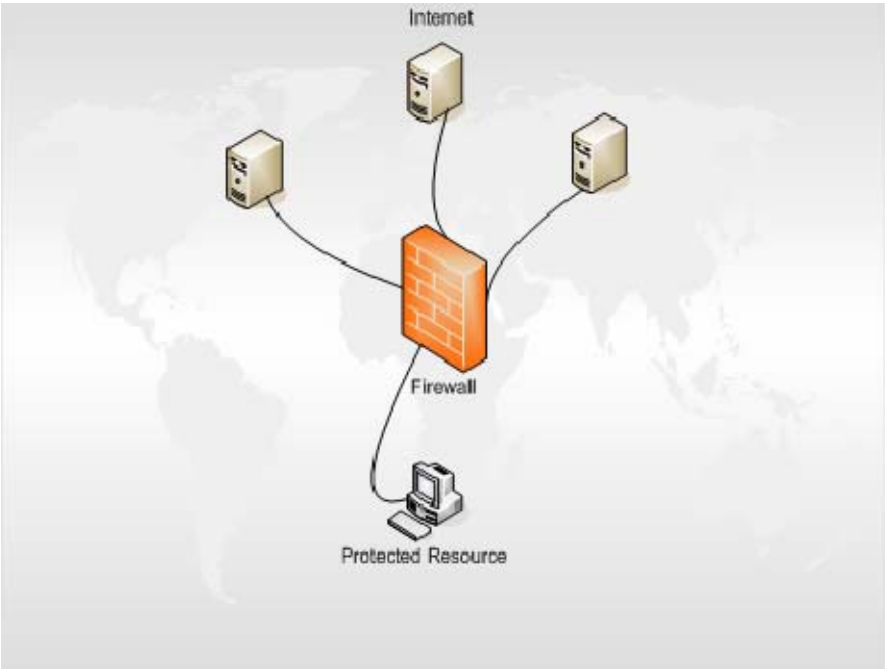
Encryption technology has come a long way over the past few years. There are more options available and solutions are better suited to business needs and protect data more effectively. Encryption applications now exist that are affordable to even the smallest organization.

D4.6: FIREWALL PROTECTION[10]

Introduction

In computer security, a firewall is hardware and/or software which functions in a networked or nonnetworked environment to prevent unauthorized communications from outside an organization from getting to the protected resources within the organization. A firewall is also used to monitor and block unsafe outbound communication with external entities. In other words, a firewall is designed to prevent dangerous communications (such as viruses or trojans) and nuisance communications (for example, "spam" e-mails), from getting inside an organization's (or individual's) networks and computers.

A computer firewall is analogous to a firewall in an automobile. In a car, the firewall protects the passengers from engine heat, noise, and fumes. In a computer network, it protects the user or network from malicious or nuisance attacks, such as attempts to inject a virus or steal protected health information (PHI). The computer firewall attempts to ensure that only authorized communications get through, whether incoming or outgoing. The firewall sits between the Internet and the computer or network that it is protecting (see diagram below). To be effective, the firewall should not only stop unwanted traffic from passing through it; it should also make the computers or network it is protecting "invisible" to outsiders.



Just a few years ago, firewalls were common only to larger organizations and high-end users. This was partly true because the typical individual user did not have high-speed access and hackers did not consider them to be worthwhile targets. In addition, the cost

[10] Neil McClenney, SEC Associates, Inc.

and technical skill required to implement a firewall was prohibitive for the average user. However, as more and more individuals moved to high speed access and the technology became less complex to implement, the dynamic of firewall implementation changed significantly. Now, firewalls are not only implemented in corporate environments, such as large insurers or health care companies, they are also found in rural hospitals, small clinics, and homes.

A corporate firewall typically includes a combination of hardware, software, and multiple detection methodologies (described below). Small office or home implementations are typically software-based and usually rely on only one of the detection methodologies. To maximize the effectiveness and efficiency of the firewall, qualified professionals should conduct a risk analysis of the environment to be protected and the anticipated threats in order to determine the "best fit" solution. Implementation of any particular strategy should be based on the criticality of the resource being protected (for example, the risks and consequences of PHI being stolen), the desired efficiency of the firewall, and the dollar cost of the implementation.

Legal Requirements

The HIPAA Security Rule, while not directly referencing firewalls, does require authentication and transmission security. Firewalls provide a method for helping to ensure that only authorized traffic is allowed on the network. It is one part of the security solution. Because they help keep unwanted traffic out (and prevent outbound communication via high-risk channels), firewalls help prevent unauthorized access to (and modification of) records on the protected system.

Given the number of firewall options, the ease of implementation of at least some firewall technology, and the scalable pricing, it would be difficult to justify not implementing firewalls as part of an overall strategy for data protection. The next section describes the three main detection methods used by firewalls, followed by a list of alternative vendors offering firewall technology.

Firewall Technologies

There are three basic methods for implementing firewalls: packet filtering, proxy service, and stateful inspection. A firewall may use one or multiple methods to implement its protection scheme. Below are high-level descriptions and examples for each type of firewall.

- In packet filtering, packets (which are pieces of data moving along the Internet) are analyzed against pre-defined filters. These filters determine which packets are allowed to get through. The packet filter may look at attributes such as the Internet Protocol (IP) address of the source, the IP address of the destination, or the originating domain name. The downside of packet filtering is that a hacker can "fake" legitimate packets and thereby penetrate the firewall. The packet filter excels, though, in speed and performance.

  - One example of packet filtering would be looking at the IP address of the source (that is, where the packet came from). Think of the IP address as the street address for the sender of postal mail. If this were a known address of a source that was not trustworthy, the IP filter could be set up to block any communication from this site. Once a packet with this source address gets to the firewall, it will be rejected and not allowed to pass through. This protects users inside the firewall from being exposed to the danger.

- In a proxy service, there are essentially two components: a proxy server and a proxy client. The client communicates with the proxy server instead of the "real" server that it needs to perform a specific action. The proxy server, in turn, communicates with the "real" server. Since the proxy server manages the communication between the end user and the "real" server, it is generally considered a more secure form of firewall than one that does only packet filtering. However, since the proxy server acts as a "middle man" in all communications, there is a penalty in terms of communications performance when compared to packet filtering.

  - It is probably easiest to think of a proxy as a managed care option for Internet communication. In an HMO, you must go to a primary care physician before you can be referred to a specialist. With a proxy server, instead of going directly to an Internet resource, the proxy server decides if you will be allowed to communicate with an external resource and then handles all of the communication once that permission has been granted. This proxy server will be configured in your web browser (eg, MS Internet Explorer). When you try to go to a website you are actually communicating with the proxy server; not the website itself. The proxy server handles the communication with the external website (assuming the proxy server's rules allow communication with the specific site). The Internet site also communicates with the proxy server, rather than directly with your web browser. This all happens behind the scenes and most users do not realize they are communicating with a proxy server instead of directly with the actual website. Thus, proxy servers can be configured with rules regarding restricted websites and restricted communication types, in order to enforce the organization's security policies.

- Stateful inspection tracks each connection traversing all interfaces of the firewall and ensures they are valid. A stateful firewall may examine not just the header information of a packet, but also the contents of the packet in order to determine more about the packet than just information about its source and destination. A stateful inspection firewall also monitors the state of the connection and other details. Because of this, filtering decisions are based not only on administrator-defined rules (as in packet filtering) but also on context that has been established by prior packets that have passed through the firewall.

  - Stateful firewalls are similar to proxy firewalls. As described in the packet filtering example, traffic moving along the Internet must have an address (eg, as with postal mail, it needs FROM and TO addresses). There is much more, however, to the packet than addressing. The information that is being passed is transmitted and received using different methods, or *protocols*. At any given point in the communication process the packets that are moving back and forth exist in different *states*. For example, in one *protocol*, there is a packet sent in a state that basically says hello, I want to talk with you. On the receiving end there is a *state* that is listening or waiting for something to communicate with it. One way of thinking about it is to think of a moderator in a debate. The moderator keeps track of the rules each participant must follow in order to speak. The participants speak to the moderator rather than to each other. In this way the moderator is in

control of the conversation. Stateful firewalls keep track of the communication method as well as the state of the packet that is passing through it. If something is not right then it can take the appropriate action.

Hardware versus Software

Firewalls can be implemented through hardware, software, or a combination of both. The decision of whether to implement in hardware or software comes down to one of cost and performance. In general, software has less up-front cost but more maintenance cost, whereas hardware has more up-front cost but less overall maintenance cost. Hardware solutions also have the least impact on system performance, but may lack the flexibility of software solutions. These are trade-offs that must be decided by the information technology (IT) staff. For the most part, it is more important to consider the features of the implementation rather than whether these capabilities are provided in hardware or software. The key is to define the anticipated threats, understand the risks, and implement the strategy that best meets the organization's policies and risk mitigation requirements. As with any aspect of system security, firewall implementation is not a one-time event. The threats are constantly changing, and the successful organization will adapt to meet those ever-changing threats.

Proper firewall configuration and maintenance is critical for both hardware- and software-based firewalls. This means setting up the rules that allow or prevent electronic communication to enter or leave an organization's network. Firewalls need to be configured based on the needs of the organization. Also, firewall configurations need to be monitored on a regular basis because risks change and the needs of the organization change. Threats to an organization do not remain static and need to be viewed, as with antivirus software, as part of an ongoing process to protect the organization from unwanted traffic. Firewalls are only as effective as their configuration. If a firewall is not configured properly, unwanted traffic is allowed through the firewall (inbound and outbound). It is not a matter of just installing a firewall. It is a matter of regular monitoring and tuning of the firewall and applying available patches so it continues to effectively protect the network and the data assets of an organization.

Firewall Product Vendors

Following is a list of vendors that supply firewall products. RTI International does not endorse any of these vendors and has not tested these products. This list is not all-inclusive, but it provides a starting point for an organization, stakeholder group, or subcontractor to locate potential vendors.

- Borderware (http://www.borderware.com/products/)
- Cisco (http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/)
- Hewlett-Packard (http://h18004.www1.hp.com/products/servers/networking/index.html)

- Fortinet Inc. (http://www.fortinet.com/)
- IBM (http://www-306.ibm.com/software/sw-bycategory/)
- Juniper Networks (http://www.juniper.net/)
- Secure Computing (http://www.securecomputing.com/)
- SonicWALL (http://www.sonicwall.com/)
- Symantec (http://www.symantec.com/enterprise/products/index.jsp)
- WatchGuard (http://www.watchguard.com/)

Summary

Computer and network firewalls provide critical security protection for computing environments ranging from a single computer in the office of a sole practitioner to large-scale enterprise networks. While firewalls should not be used in place of antivirus and antispyware software, a well-tuned and updated firewall can do much to prevent malicious and nuisance software from reaching protected resources. Firewalls can also prevent unauthorized data transmission out of an organization. There are several types of firewall technology available, and their proper configuration can be complex. It is best to use knowledgeable IT resources to ensure that the organization has the right firewall for its mission, with proper configuration and maintenance procedures in place.