

HIPAA Technical Brief

Understanding the Requirements and How To Address Them

October, 2007





Table of Contents

HIPAA and Network Security_____	3
HIPAA Requirements_____	4
<i>Privacy</i> _____	4
<i>Security</i> _____	4
<i>Access Control</i> _____	5
<i>Audit Control</i> _____	6
<i>Integrity</i> _____	6
<i>Person or Entity Authentication</i> _____	7
<i>Transmission Security</i> _____	8
Summary_____	8



HIPAA and Network Security

Over the past several years, the methods by which health care organizations manage information have changed. Federal and State regulations have introduced provisions to ensure record keeping moves to an electronic medium. This change to electronic storage allows for more portable information to be easily shared between health care entities. Consequently, this ease of access also requires security improvements to ensure data is not improperly available or inadvertently or purposely modified by unauthorized parties. The Health Insurance Portability and Accountability Act of 1996 (as amended) (HIPAA) has imposed heightened security requirements on health care organizations and their related entities who maintain health care records.

HIPAA was enacted to: (1) Protect the health insurance coverage of workers and their families when they change or lose their jobs (portability); and (2) protect health data integrity, confidentiality and availability (accountability).

HIPAA applies to covered entities that transmit any health information in electronic form in connection with a transaction covered by HIPAA. Covered entities include: (1) government and private health plans, insurers, and administrators; (2) hospitals, physicians, and other health care providers; (3) some employers; (4) clearinghouses; (5) valued added networks (VANs); (6) billing agents; and (7) other service organizations.

The Department of Health and Human Services (DHHS), which governs HIPAA compliance, has explained the purpose of the Privacy Regulations of HIPAA as follows:

1. To protect and enhance the rights of consumers by providing them access to their health information and controlling inappropriate use of that information
2. To improve the quality of health care in the U.S. by restoring trust in the health care system among consumers, health care professionals, and the multitude of organizations and individuals committed to the delivery of care
3. To improve the efficiency and effectiveness of health care delivery by creating a national framework for health privacy protection that builds on efforts by states, health systems, individual organizations and individuals

HIPAA

(1) Protect the health insurance coverage of workers and their families when they change or lose their jobs (portability).

(2) Protect health data integrity, confidentiality and availability (accountability). HIPAA applies to covered entities that transmit any health information in electronic form in connection with a transaction covered by HIPAA.

Covered Entities

- Government and private health plans, insurers, and administrators
- Hospitals, physicians, and other health care providers
- Some employers
- Clearinghouses
- Valued added networks
- Billing agents
- Other service organizations



HIPAA Requirements

Two primary provisions of HIPAA that apply to covered entities are Privacy and Security.

Privacy

Under the Privacy Regulations of HIPAA, covered entities may not use or disclose an individual's protected health information (PHI) except as permitted or required by the regulations. Additionally, an individual has the right to receive an accounting of disclosures of his or her PHI made by the covered entity in the past six years (although not prior to the compliance date). A covered entity must establish policies and standards to comply with these regulations. Generally, three concepts should be observed when evaluating HIPAA compliance:

Privacy

Covered entities may not use or disclose an individual's protected health information (PHI) except as permitted or required by the regulations. Additionally, an individual has the right to receive an accounting of disclosures of his or her PHI made by the covered entity in the past six years.

1. To protect and enhance the rights of consumers by providing them access to their health information and controlling inappropriate use of that information
2. To improve the quality of health care in the U.S. by restoring trust in the health care system among consumers, health care professionals, and the multitude of organizations and individuals committed to the delivery of health care
3. To improve the efficiency and effectiveness of health care delivery by creating a national framework for health privacy protection that builds on efforts by states, health systems, individual organizations and individuals

These standards allow companies great flexibility for choosing the method for HIPAA privacy compliance. They do not mandate the use of any specific technology. Instead, HIPAA urges entities to recognize their security risks and implement the solutions they deem appropriate for their respective environments.

Security

The Security Regulations section of HIPAA sets forth the security objectives that covered entities must meet. These include:

1. Access Control: No access may be attained by someone who is not authorized
2. Audit Control: All access must be tracked and logged
3. Integrity: No data can be altered or destroyed in an unauthorized manner
4. Person or Entity Authentication: Corroboration that an entity is who it claims to be
5. Transmission Security: Mechanisms are in place to guard against unauthorized access to data transmitted over a communications network

Virtela's network solutions can help health care organizations and other entities address these security requirements and build trusted relationships between health care customers, employees, businesses, trading partners and shareholders. The following sections explain how.



Access Control

Access control requirements ensure only those individuals with proper authorization have access to data. Through the use of layer-2 networks, such as switched Ethernet, frame relay, ATM, private line, Multi-Protocol Label Switched (MPLS) or encrypted IP VPN networks, access is defined by physical connectivity. As long as there is physical security to protect each network access point, the network retains strong access control.

Access Control

Access control requirements ensure only those individuals with proper authorization have access to data.

Closed layer-2 networks, despite the inherent security, are becoming less common. The Internet is fast becoming the chosen medium for wide-area networking (WAN). Additionally, although most Local Area Networks (LANs) use layer-2 switched Ethernet, there has been exponential growth in wireless network access adoption within the LAN. The use of wireless, combined with the nearly ubiquitous presence of the Internet, drastically reduces the inherent access controls afforded by layer-2 networks. Strong physical security no longer assures network protection, and meeting the required goals of HIPAA Access Control requires supplemental security.

The first line of defense is a good firewall and firewall policy. Both are necessary and neither is effective without the other. A \$100,000 firewall on a DSL line will not provide adequate protection if the security policies are not well considered.

Firewalls define which nodes may transmit data, what type of data it can be, and to what destination it is permitted. Firewalls inspect all data that passes through them and block all traffic lacking proper permissions. These restrictions address a significant portion of the access control requirements. Going a step further, firewalls may be combined with user authentication, including two-factor authentication such as RSA keys or digital certificates. Use of these tools ensures authentication of the user before access is permitted. Two-factor firewall authentication allows comprehensive logging of resource access and user activity.

Virtela delivers comprehensive firewall services on industry leading firewall platforms. Virtela fully supports Juniper/Netscreen, Cisco and Checkpoint firewalls. Service deployments include a thorough examination of the network and our Sales Engineers have comprehensive checklists to collect the information required for a successful and secure service deployment.

Virtela's life-cycle management maintains the viability of firewalls through the ever-changing security landscape. As new threats are discovered, new patches or updates released, and new methods of configuration proposed to properly defend against threats, Virtela maintains the knowledge to implement the required changes. Virtela automatically applies configuration changes and updates in compliance with security best practices. Customers can rest assured that Virtela will not miss a new vulnerability and will properly configure managed devices in response to emerging threats.



Audit Control

The purpose of having electronic resources is to simplify access to records for authorized users. Tracking the access of each user is mandatory for HIPAA compliance. Auditing controls must trace all data changes. When a request is made to have a covered entity amend PHI, HIPAA mandates tracking of the change, the time of the change, and the identity of who made that change. Audit controls also identify unauthorized access attempts and help identify those responsible.

Audit Control

Auditing controls must trace all data changes. HIPAA compliance mandates the tracking of each change, the time of the change, and the identity of who made each change.

Audit controls are most applicable to resources, generally considered as the server housing the data. Auditing services are also integral to the network, and the strongest auditing tools combine the use of both. Resource auditing includes the scrubbing of server event logs, access attempts, and data manipulation on monitored files. Auditing resources can be further enhanced through the use of auditing software tools, such as Tripwire.

Network auditing enhances resource auditing controls. For a detailed understanding of what modifications may have been made, and when, services like Intrusion Detection/Prevention Services (IPS) are available. IPS performs deep packet inspection to recognize exactly what is occurring with each packet sent through the IPS. IPS management services monitor the traffic and generate detailed logs of every data access request passing through the sensor. Combining the capabilities of both resource based and network based knowledge are IPS software clients. These tools are installed on the resources to inspect and log each packet entering the resource. IPS network and resource based tools can actively block unauthorized or misbehaving traffic, and ensure detailed logs are collected against authorized access.

Virtela provides complete management services for network or resource based IPS. Virtela supports hardware and software platforms from Juniper, Cisco and 3COM/Tipping Point. Throughout the IPS life cycle, Virtela continuously evaluates new threats and vulnerabilities, applies updates and patches as required to maintain tight security and historical logging of audited services. This level of auditing ensures unparalleled data protection and demonstrates compliance against HIPAA standards.

Integrity

Integrity is the assurance that data has not been modified in an unauthorized manner. In relationship to the network, integrity means that data sent from the source is exactly the same as the data reaching the destination. In relationship to data on the resource, integrity means that no modifications have been made by any person or entity who is not explicitly authorized to do so. Network integrity is verified through the use of technologies such as CRC checksums, which validate that data has not been altered in transit. File integrity can be validated by similar principals using MD5 signatures. MD5 ensures that the present signature of a file matches the expected signature; a mismatch indicates an altered file.

Integrity

The assurance that data has not been modified in an unauthorized manner and that no modifications have been made by any person or entity who is not explicitly authorized to do so.

Network integrity services protect against “man-in-the-middle” attacks or “IP Spoofing,” where an



unauthorized party intercepts a message, modifies the data, and then sends it on to its intended recipient. The recipient is unaware the data has been modified and treats it as though it were sound.

Ensuring the integrity of network communications requires a different tactic than the services provided by firewall or IPS monitoring. Integrity is best addressed through encrypted VPN services. An encrypted VPN scrambles data to ensure that only users who may make use of the data are the sender and the recipient. Encrypted data cannot be unscrambled without the proper “key”. Any communication captured in transit is unusable as the encryption garbles it beyond recognition until its unique key is applied.

For encrypted VPN services, Virtela is unmatched. Virtela has been enabling global VPN networks as a core competency since its inception in 2000. Whether for secure communications between VPN peers across the planet or within a business park, Virtela can establish encrypted VPN connectivity between any two supported devices. Real-time monitoring is performed on each Virtela VPN to immediately identify and react to service issues.

As new service locations and resources are added to the network, Virtela will update them as desired. The combination of VPN services with the auditing and access controls of firewall and IPS services significantly enhances the overall security posture of a company.

Person or Entity Authentication

Authentication services validate a user’s identity. Standard Person/Entity Authentication assigns each entity an account that provides a designated level of access. The account is matched to a password that validates the entity’s identity, proving the person/entity is who they claim to be.

Person or Entity Authentication

Authentication services validate a user’s identity. That the person or entity can be trusted to be who they claim to be.

Resources within a network perform the majority of Person or Entity Authentication. Using the example of a Microsoft domain, a user’s account defined within Microsoft’s Active Directory (AD) will validate a person or entity’s rights to request or access data. Upon logon to the domain, that person receives the rights specified for his/her account, and those rights are verified against each new resource request before access is granted.

Networks may also perform Person or Entity Authentication. When a user attempts to establish a VPN connection over the Internet, that access is not permitted until the person has identified himself as a valid user and provides the proper credentials. Such validation can be enhanced through the use of a two-token configurations, where the user must provide at least two methods of confirmation to receive network access. Most two-token authentication tools make use of the user account, their password and either a digital certificate or an Access Key-FOB such as that provided by RSA.

Virtela supports both site-to-site (peer) and end-user VPN connectivity through either SSL or IPSEC technologies. Two-token authentication is supported through the use of RSA key-FOBs. Through the established expertise of Virtela’s VPN solutions, covered entities may easily establish demonstrable Person or Entity Authentication sufficient to meet and exceed HIPAA requirements.



Transmission Security

Transmission security requires that mechanisms be in place to guard against unauthorized access to data as it is transmitted across a network. Transmission security can be met through the use of closed networks, such as ATM, frame relay, private line and MPLS-VPN. To ensure the network is closed, all access points must be physically secured from any possible unauthorized access and have no connectivity to unsecured networks. As this is generally unrealistic in all but the most security-conscious networks, Transmission Security is another objective which requires encrypted VPN services.

Transmission Security

Mechanisms to guard against unauthorized access to data as it is transmitted across a network.

Encrypted VPN services are in effect strong security service for secure Internet connectivity, and the same services that guarantee network data integrity as it passes over the Internet. For highly sensitive information, such as PHI records, encrypted VPN's should be used to secure all data as it passes between peers.

Summary

The requirements set forth by HIPAA contain significant restrictions that must be observed by covered entities. As a global provider of IP VPN networking and managed security services Virtela can help covered entities meet the HIPAA challenges.

The growth of Internet usage in the communications between covered entities, their partners, and the health care recipient mandate that secure methods be implemented to secure the data, both in transit and at rest. Enabling the convenience of health care record sharing between a doctor in Tennessee who's suddenly treating a patient from Seattle injured on vacation, means that tight safeguards must be established to keep those records from being inappropriately handled.

Virtela's suite of Managed Security Services meets or exceeds the compliance requirements for each of the following:

1. Access Control - Firewall: Permit communications only for those with authorized access
2. Audit Control - Firewall, IPS: Restrict and log all data sessions to managed resources
3. Integrity - VPN: Encrypts the data passing between peers, nullifying ability to alter in-route
4. Authentication - VPN, Firewall: Entities must authenticate to attain network access (VPN) and authenticate to pass data (Firewall)
5. Transmission Security - VPN: Encrypts the data, nullifying the ability to alter in-route. Provides monitoring to ensure encryption services are functioning

Virtela further enhances this suite of services with fully customizable Professional Services. Virtela Professional Services creates custom solutions as desired to meet any potential business objective.