



The Twelve Most Common Threats to HIPAA Compliance When Providing Remote Access to Systems and Data

March 2010



The Twelve Most Common Threats to HIPAA Compliance When Providing Remote Access to Systems and Data

Backdrop

On August 12, 1998, the Department of Health and Human Services (HHS) published a proposed rule to establish minimum security of electronic health information.

Technology has evolved significantly in the years since that rule was first proposed, including:

- Widespread use of the Internet in standard business practices.
- Availability of Internet-based remote access and support products.
- The emergence and acceptance of open source software within the enterprise.
- The adoption of digitally-based diagnostic devices and data collection systems allowing patient information to be stored in a digital form at the point of collection.
- The evolution of portable wireless devices making them more capable to access, store and display patient data.

This evolution, and the business practices that use this technology, may cause organizations to violate either to spirit or the letter of the HIPAA regulations.

Threats to HIPAA Compliance

Here are some new threats to the HIPAA regulations:

§164.306(a)(2) Security standards: General rules.

Protect against any reasonably anticipated threats or hazards to the security or integrity of such [health] information.

§164.306(a)(3) Security standards: General rules.

Protect against any reasonably anticipated uses or disclosures of such [health] information that are not permitted or required...

The above two regulations are related. They both address the need to protect against threats to the security, integrity and disclosure of health information. Technologies such as the Internet and products such as WebEx, GoToMyPC and VNC provide faster, cheaper and more immediate access to information. While they each can provide real benefits, they also threaten HIPAA compliance in a significant way.

Any product that provides access that is not encrypted violates these general rules. Many versions of VNC, for example, are not encrypted.

Any product that does not log remote access to systems or applications violates these general rules. Most versions of VNC provide no logging functionality. And while products such as WebEx and GoToMyPC perform logging, they can have multiple logs of access to the same systems making it difficult or impossible to track.

Threats to information security can also occur when an employee leaves a company, or their responsibilities change. The ability to quickly change access rules or change passwords for all systems affected is essential to mitigating this threat. Many remote access solutions store their passwords on the local system. This makes changing passwords quickly very difficult and time consuming leaving systems exposed to unauthorized access.

Third party hosted access solutions such as WebEx and GoToMyPC/GoToAssist by their very nature make it very difficult, if not impossible to control access. Their primary advantage in the marketplace is due to the fact that they provide ubiquitous and immediate access. While

convenient, it can pose a significant threat to HIPAA compliance. Unless a company blocks access to these services, any person inside the organization can open an account with a 3rd party service and thus provide unrestricted access to any system on the network. Since access is not centrally controlled, there is little to no means available to stop access when threats to information occur. This, coupled with no centralized access logging, makes these types of services a clear threat to HIPAA compliance.

§164.308(a)(1)(ii)(D) Administrative safeguards: Information system activity review.

Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

Any remote access solution that does not log access is clearly in violation of HIPAA regulations. VNC is the most obvious threat. However, many other remote access solutions that do provide local logging can still violate the spirit, if not the letter of the law. In an organization with many systems, local logging can provide little if any protection against threats to health information security and integrity. This is especially true in large organizations with hundreds or thousands of systems. It is nearly impossible to monitor and control access when the logs are stored locally. That would require many man-hours of work on a continuous basis to gather these logs and review them for access violations. The end result is that typically this function would not be done. A method that centrally logs access to all decentralized systems provides a means to more readily monitor access and insure compliance.

While 3rd-party services do provide a centralized logging mechanism for all access that takes place from their services, it also suffers the same flaws that come with locally logged methods. Since any number of people within an organization can have accounts, there can be more than one central log that exists. Only when all accounts can be known with certainty is compliance assured when using these services.

§164.308(a)(3)(i) Administrative safeguards: Workforce security.

Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information...and to prevent those workforce members who do not have access...from obtaining access to electronic protected health information.

Any system that stores passwords locally can violate this regulation. This is particularly true of organizations with many systems since it would be virtually impossible to restrict access in a timely manner. This will leave information exposed to unauthorized access while administrators scramble to complete the very time consuming task of changing passwords on each system.

Technologies such as VNC can violate this regulation since it stores passwords locally. Surprisingly, even common remote access methods to most UNIX and LINUX systems can violate this regulation. Remote access programs such as telnet and ssh store their passwords locally. Changing these passwords quickly is all but impossible when there are many systems involved. Even dial-up access to systems can violate this regulation since dial-up passwords are typically stored locally.

An access solution that supports centralized access control methodologies such as NTLM, Active Directory, or LDAP is much more compliant. These methodologies allow for rapid changing or shutting down access to all systems, local or remote.

§164.308(a)(3)(ii)(C) Administrative safeguards: Termination procedures

Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends...

Termination of employees can leave systems exposed to unauthorized access. This is particularly true with Solution Providers since most of the systems they support are remote systems. Remote systems by their very nature can be a challenge to manage and control access. When an employee leaves a Solution Provider, they take with them a cache of proprietary information include passwords, modem phone numbers, and access methods. As with regulation §164.308(a)(3)(i), any access method that stores passwords locally, or uses locally controlled authentication, is likely to be non-compliant. In these situations, a terminated employee can leave a Solution Provider and still have access to the remote systems that Solution Provider supports. This is clearly a HIPAA violation. This is particularly true of systems that are accessed via dial-up since most dial-up systems are assumed to be secure since they don't use a public network to provide access. However, because passwords are stored locally, changing passwords quickly to insure compliance can be all but impossible. This is further exacerbated by the fact that often the same administrator password is used for all remote systems for convenience. Thus, knowing one administrator password will typically provide access to any remote system.

An access method that provides access authentication centralized on the Solution Provider's network resolves all the above mentioned compliance issues.

§164.308(a)(4)(ii)(B) Administrative safeguards: Access Authorization

Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.

§164.308(a)(4)(ii)(C) Administrative safeguards: Access establishment and modification

Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

These two regulations are closely related. Access control is a critical requirement for HIPAA compliance. Any access control method that is not centrally authenticated is highly vulnerable to violating compliance because they are very difficult to change, stop, or control access. This is true of many of the most common remote access methods including PCAnywhere, VNC, WebEx, GoToMyPC, telnet, ssh, and dialup.

To insure compliance, a means of centralizing authentication at the Solution Provider level is required. This will allow the Solution Provider to rapidly and completely control access to all of the remote systems entrusted to their care.

§164.308(a)(5)(ii)(B) Protection from malicious software

...Procedures for guarding against, detecting, and reporting malicious software.

The emergence and acceptance of open source software makes it particularly difficult to monitor and prevent its installation. Since it is available at no cost, the typical purchase justification and security control processes can easily be subverted. An open source software technology of particular concern is VNC (Virtual Network Computing). VNC allows for the remote access and control of computers. VNC is readily available, easy to download, and easy to install. Unfortunately, VNC lacks the most basic of security features making it a “backdoor” for anyone looking to hack into a computer. Here’s how:

- Passwords are stored locally.
- Most versions allow unlimited password attempts, making it ready target for brute force password breaking.
- The data stream is not encrypted, including passwords.
- The software can be readily changed to operate without anyone’s knowledge that it is running on the computer.
- No logging is done of any access activity or attempts.
- No integration with standard access control systems such as Active Directory or LDAP.

More concerning still is the fact that the source code is freely and widely available for VNC. For a hacker, this provides a virtual “roadmap” of how to hack into a system that is running VNC. A hacker can use this source code to find out where and how the passwords are stored so they can be overwritten. They can use this source code to determine the communications protocol making it easy to intercept and interpret the activity taking place on a computer running VNC. They can also use this source code to determine how to change the VNC settings to make its operation invisible to the user whose computer it is running on.

For all of these reasons, VNC should be considered malicious software as defined by the HIPAA rule.

§164.310(a)(1) Standard: Facility access controls.

Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

The emergence of web-based meeting and support solutions provides a particular challenge to HIPAA compliance. These types of solutions provide a simple means to provide access over the Internet to a particular computer. These solutions typically do not require any pre-installation of software. Further, these types of solutions operate using firewall ports that are typically open for normal web-based traffic (i.e. Port 80). Often they are sold on a subscription basis at a relatively low monthly cost. This allows their ready use without drawing the attention of the procurement staff. All of these factors combine to allow undetected, unauthenticated, and unmonitored access to electronic healthcare information.

As defined in this rule, there should be policies and procedures in place to limit the “physical access” to electronic information systems. At the time of the HIPAA rule’s creation, that almost always meant a person being physically present at the computer where the information was stored. The emergence of these web-based remote access technology has created an environment that provides ready access to the physical computer without having to be physically present.

These types of web-base remote meeting and support solutions should be restricted based upon the intent of §164.310(a)(1).

§164.308(a)(5)(ii)(C) Standard: Security Awareness and Training.

Log-in monitoring (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies.

The widespread use of networking and the Internet provides much more ready access to computers. This creates vulnerabilities when attempting to monitor log-in attempts and reporting any suspicious activity or failed logins. Most UNIX and Linux-based systems allow for dial-up, telnet or ssh connections. These connections, if they track login activity, do it locally to the system being logged into. Local logging makes it very difficult to continuously monitor login activity in order to react to unauthorized access or hacking attempts, thus these types of systems are at significant risk for not being HIPAA compliant. This is especially true of systems that are accessed via dial-up modem since these systems are disconnected from any type of central network making access to logs in a timely matter all but impossible.

Any system that allows direct dial-up access is violating the standard set by this rule because it provides no means to readily monitor or report login activities and discrepancies. Further, any system that tracks login activity locally can cause a compliance threat because the logs are not centralized and aggregating the logs to allow for easier monitoring is prone to not be done because it is time consuming or expensive.

§164.308(a)(5)(ii)(D) Standard: Security Awareness and Training.

Password management (Addressable). Procedures for creating, changing, and safeguarding passwords.

Since the HIPAA regulations were first drafted, an ever larger number of distributed computers have been installed. The sheer number of computers, installed in an ever increasing number of locations, makes compliance ever more difficult.

Any application or operating environment that stores passwords locally is a threat to HIPAA compliance. This is particularly true for UNIX and Linux systems that store passwords locally. The low cost of computer hardware has created a situation where these types of systems have proliferated, particularly in doctors' offices and clinics. Any healthcare provider that has multiple locations, or hosts multiple computers, is at heightened risk for noncompliance. Many times the same password is used on multiple computers. While this makes it easier for systems administrators to access multiple computers without having to remember a separate password for each, it makes it very difficult to insure compliance. Changing passwords frequently, and upon significant security events (e.g. employee termination), is critical to insuring security and data protection. Since each computer stores its passwords locally, each computer will have to be accessed in order to change its password. If the number of computers is relatively small, this is not an issue. However, when the number of systems is large, this is very difficult to manage. The end result is that compliance to this standard is at risk.

Any system whose access is not managed by a centrally controlled authentication process is at risk for noncompliance.



The Twelve Most Common Threats to HIPAA Compliance When Providing Remote Access to Systems and Data

§164.308(a)(6)(i) Standard: Security incident procedures.

Implementation specification: Response and Reporting (Required). Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.

The same threats to compliance exist for this regulation as it does for §164.308(a)(5)(ii)(D). In addition, this rule addresses the requirement to respond to suspected or known security incidents, to mitigate them and to document them and their outcome. Decentralized authentication and security models make compliance to this rule very difficult, if not impossible.

Centralized authentication and security models allow not only better control of access, but also provide a better means to collect security data for forensic purposes.