HIPAA
Remote Access Compliancy

Many healthcare providers are questioning the validity of Federal compliancy due to the Health Insurance Portability and Accountability Act of 1996. The law has a very broad impact over many operations of the healthcare industry. The following white paper provides an analysis of current HIPAA regulations that are impacting the healthcare IT industry. Specifically, this document discusses vulnerabilities associated with remote control software and provides a solution for secure remote access over a HIPAA compliant network infrastructure; designed to preserve the confidentiality of patient records.

Contents

CrossTec Corporation
500 NE Spanish River Blvd.
Boca Raton, FL 33431
800-675-0729
www.CrossTecCorp.com

HIPAA
Remote Access Compliancy

The Health Insurance Portability and Accountability Act of 1996 has many healthcare providers questioning the validity of the compliancy of the organization as the law has a very broad impact over many operations of the healthcare industry. The following white paper provides an analysis of current HIPAA regulations that are impacting the healthcare IT industry. Specifically, this document discusses vulnerabilities associated with remote control software and provides a solution for secure remote access over a HIPAA compliant network infrastructure that is designed to preserve the confidentiality of patient records.

## 1.	Remote Compliancy

Since the Health Insurance Portability and Accountability Act of 1996 (HIPAA) was established, healthcare providers have gone to great lengths to comply with its requirements. HIPAA, the largest act to affect U.S. business since the Americans with Disabilities Act, revolutionized the way healthcare providers conduct business. IT departments in particular have made significant changes to comply with HIPAA requirements, and under HIPAA regulations, healthcare providers are legally obliged to safeguard all patients' medical records against nonconsensual access or authorization.

This places new significance on IT departments' responsibility to protect the corporate network. Adequately securing information is crucial to ensure and protect company data, whether it is stored on a network, server, or individual machines. One breach of security resulting in the unauthorized disclosure of Protected Health Information (PHI) can be detrimental to patient confidentiality. Leaked PHI has the potential to publicly humiliate patients or even make them susceptible to discrimination, punishments, scrutiny, and blackmail.

However, the patient is not the only entity who's subject to repercussions. Health providers face the possibility of damage to their public image, losing credibility amongst their community and colleagues, and suffering a loss of clientele. Worse yet, health providers found guilty of inadequately safeguarding PHI, regardless of intent, are subject to fines of as much as $250,000, jail sentences up to 10 years, and even law suits from patients who have endured damages.

Remote control software is an example of an application that is widely used amongst the IT industry to remotely access distant machines. Remote control software acts like a giant extension cord stretching from a users' keyboard, mouse, and monitor to another computer at a different location. Using remote control technologies, a user can control the desktop of a distant computer with their own keyboard and mouse, just as if they were seated at that distant computer. To preserve the confidentiality of PHI, IT departments must take every precaution to secure all data streams, utilities, and points of entry used to access external machines via the Internet.

In the corporate environment, remote control software is used by IT professionals to troubleshoot end user computers as well as employees telecommuting from home to the office. Unfortunately, remote control software often creates vulnerable points-of-entry into the network when sufficient security is not implemented to protect all remote control sessions.

2.   Secure Remote Connections
There are several communication components that must be secured in order to protect PHI. For instance, the Client software must be present on all computers involved in a remote control session as the Control application controls the application installed on the end user's machine. The Client application operates on the controlled machine, enabling the Control to establish a connection to the Client and control activities on the machine. Once a connection is established, the data is streamed between the two machines to enable the Control to take over the Client.

In order to protect a remote control session, all data streams must be secured and Control and Client access must be restricted to authorized users. The developers of CrossTec Remote Control took this and much more into consideration when they designed CrossTec as an enterprise remote control utility. CrossTec has been designed around customer feedback, suggestions, and needs; resulting in a highly comprehensive enterprise solution for securely accessing and controlling remote, cross-platform machines. Recognizing the importance of protecting corporate data, the developers took security very seriously when designing CrossTec Remote Control. In fact, no other remote control application provides as much security as CrossTec Remote Control. Let's take a look at how CrossTec facilitates a HIPAA compliant network infrastructure by restricting Control and Client access and protecting data streams.

3.   Centralized Security Management
CrossTec Remote Control utilizes Windows Active Directory (AD) to enable an administrator to centrally manage all users' access privileges, machine rights, unique user IDs, and passwords. A remote control application that does not let an administrator use the centralized authentication tools they already use on a daily basis, such as AD Users and Computers, is at a disadvantage by introducing additional management consoles to provide the same functionality. Each AD Group is assigned privileges pertinent to the job responsibilities. For example, some IT employees need access to all applications and computer information in order to troubleshoot end users when problems arise, while other supervisors may have limited access to only monitor his/her employees, so they do not need remote control functionality. By limiting the Control's access privileges, a network administrator can restrict who has access to confidential documents such as patient records and other PHI.

Corporate networks are typically layered with tight security to protect confidential data. For instance, the common perimeter and desktop firewalls restrict network traffic to specified ports and applications. Unfortunately, these are also the same communication doorways that attackers use to gain access to private networks. This is why many IT departments work very hard to minimize the number of ports that are opened on their network, because the more ports that are open, the easier it is for an attacker to break into a network. With remote control software, a port must be opened to transmit data between two machines participating in the remote control session.

CrossTec developers recognized this long ago and realized the inherent security risk, so they created the CrossTec Gateway Server to resolve this issue. The CrossTec Gateway Server acts like a traffic patrol officer, directing network traffic through a designated port to enable network administrators to define a specific port for all remote access communication, usually HTTPS (443), an encrypted TCP port. Therefore, no additional ports are opened to expose the private network to outside attackers.

Unfortunately, due to an ever increasing number of security threats, nothing is a sure thing. So what happens if an attacker manages to break into your network? All they need to do is pirate a Control computer and access every Client machine on the network. CrossTec Remote Control restricts access to Clients machines, so network administrators can rest assured that even if an attacker were able to

commandeer their computer, they would not be able to remotely connect to Client machines containing PHI or other important data, even if they had an administrator password.

4.   Restricting Remote Access
If machine passwords have been assigned, Control users are prompted for a password that will either grant or deny them access to the Client machine(s). These passwords can be assigned individually to give each computer a separate password for every Client machine. Control's access security can also be integrated into current network authentication schemes such as Active Directory, or local Windows security.

The CrossTec Client can be configured a number of different ways to give the Client's user complete control over whoever is trying to access their machine, so whoever is using the Client machine ultimately determines how access to the Client will be configured. For example, if a CEO is working with the Client computer, he/she may want to be able to restrict who and when someone is accessing their machine. However, a sales rep whose Client machine is monitored by their supervisor will not need to know when they're being monitored or who is monitoring them.

CrossTec's authentication feature alerts the Client's user when a Control attempts to connect to their machine. The Client can grant or deny Control access at their discretion because CrossTec enables Clients to be configured to only accept remote connections from a designated list of users. By creating Profiles on the Client machines and associating these Profiles to AD Groups it becomes easy to create multiple sets of permissions depending on which Windows AD Group member is controlling the Client. This allows an administrator to assign remote control permissions for the Help Desk group that are lower than those of the Domain Admins group when connecting to the same Client for example.

5.   Serial Keys
For further Client restriction, CrossTec developers offer a Serial Key feature to organizations when purchasing their licenses. Customers who choose to implement a Serial Key create a unique password that is embedded in every license they deploy, so only Controls with the correct Serial Key can access Clients with the unique embedded password. This proves beneficial for preventing outside users from gaining access to the company network via a separately purchased CrossTec Remote Control application or a trial license. For instance, if an IT employee is fired from a company, they still have knowledge of company passwords and the whereabouts of confidential information. All they need to do to hack into the network is install their own CrossTec Control and access the Client machines using the company's passwords for clearance. If the employer deployed a Client configured to use Serial Keys, the dismissed employee lacks the unique embedded password on the Control and is not allowed access to the Client machines of the employer even if they have the correct Windows credentials.

Information on a hard drive can be protected with firewalls and virus scanners. However, once that information leaves a computer to travel through cyberspace, it has the potential to be accessed and possibly manipulated. Any attacker could essentially intercept the data in transit and access PHI.

A doctor who remotely accesses patient records poses the risk of leaking that information to unintended parties, so it is extremely important to encrypt all data that is transmitted over the Internet. CrossTec Remote Control provides the highest level of encryption in the remote control software industry. Encryption is the process of converting data into an incomprehensible form and ensures that any efforts to interpret intercepted transmissions will fail. Every CrossTec connection is protected with the government standard 256-bit AES encryption, the most current way to securely transmit data over the Internet.

6.   Accountability

When using remote control software on a network, information is constantly being accessed by numerous individuals. In the event of an intrusion, it is nearly impossible to identify who accessed what information without the ability to log remote sessions. With CrossTec, every Client logs and documents all Remote Control activity to the Event Log of the Clients machine. This is beneficial for investigating intrusions or suspected malicious activity, but experienced hackers can simply go in to these local logs and erase their footsteps so there is no record of them ever being on the Client machine.

The CrossTec Client can provide a solution in this scenario by centrally logging all activities to a secure location that is password-protected. Therefore, attackers cannot erase their footsteps without the mandatory administrative password used to access the protected activity log on the network. With the government enforcing strict punishments for corporate HIPAA violations, pinpointing a guilty party may shift the blame from the entire corporation to the specific individual who committed the act.

7.   Summary

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) forever altered the way healthcare is practiced in the United States. Its reforms impacted the internal and external operations of the healthcare industry by protecting both employees and patients under Federal law. While HIPAA regulations are not entirely IT related, information security plays a vital role in the overall compliancy of a healthcare provider. In fact, two of the four main objectives of HIPAA are directly related to information security, including the reduction of fraud and abuse and the safeguarding of Protected Health Information. Healthcare providers found guilty of fraud or not maintaining the confidentiality of their patients' PHI are subject to fines of as much as $250,000 and jail sentences up to 10 years.

Unfortunately, there has been no official outline established for a secure network infrastructure designed to preserve PHI and reduce fraud. Each healthcare provider is responsible for instituting their own steps for developing and maintaining a HIPAA compliant network infrastructure. Experts recommend healthcare providers to conduct security audits and penetration tests to identify potential vulnerabilities on their network. Once identified, these vulnerabilities can be eliminated with additional security or the replacement of non secure applications that may pose a threat to network security.

Remote control software is one type of application that has the ability to threaten the privacy of PHI by creating network vulnerabilities. Remote control applications are widely utilized amongst IT departments for saving time, money, and the end user from wasted hours of down time by minimizing time for software support. Having the embedded security to protect remote control sessions ultimately determines the compliancy of the implementation of the product. When selecting remote control software for a healthcare environment, confidentiality is the most important feature for assuring HIPAA compliancy.