What is HIPAA?
Organizations that must adhere to the Health Insurance Portability and Accountability (HIPAA), know that encryption is now a de facto primary aspect of HIPAA compliance after the passing of the HITECH Act.

There are a couple of reasons for this increased focus on encryption.

First, the U.S. Department of the Health and Human Services (HHS) issued guidance wherein “unsecured protected health information (PHI)” is essentially any PHI that is not encrypted or destroyed. Under this definition, it doesn’t matter how many chains, walls, doors, biometric gizmos and guards with lethal weapons you have at your service. As long as PHI is not encrypted, it is considered unsecured.

A second and more compelling reason why encryption is now a requirement is the introduction of HITECH’s breach notification initiative, which requires HIPAA-covered entities to send notification letters if there is a breach of unsecured PHI. However, as HHS pointed out, the use of encryption grants safe harbor in the event of a breach because encrypted PHI is not unsecured PHI.

Oddly enough, in the same breath, HHS also notes that “covered entities and business associates are not required to follow the guidance.” However, cleaning up the mess behind a breach notification can cost millions of dollars, so one would have to be supremely confident – or reckless – in not taking advantage of the encryption safe harbor. With such mixed signals, though, it is not hard to see why encryption is called a de facto requirement.

What type of encryption is required?
In the past, companies offered hard drives that used strong encryption. However, analysis showed that strong encryption was used but only to protect the password and not the data that was stored on the devices. The actual data stored on the hard drive was encrypted with an encryption algorithm developed by the company, which proved to be anything but strong.

This illustrates the potential pitfalls of choosing any type of encryption package – a lack of strong, secure encryption. Obviously, some applications do a better job of protecting data than others, but how can a company choose the right one?

HHS does not provide any guidance in this area. Instead, HHS defers to the National Institute of Standards and Technology (NIST) to direct organizations to a number of special publications on the subject.

While these requirements are for federal agencies, they could also serve as a great guide for private practices. Since HHS deferred to NIST when it comes to encryption, companies need to meet the expectations of what NIST considers “proper” encryption for sensitive data.
HOW NETOP REMOTE CONTROL MEETS THEM

Centralized 2 and 3 Factor Authentication

Netop Authentication via Security Server
The Netop Security Server verifies the Guest identity against the database service that holds all the pre-defined Guest IDs and passwords.

Windows Authentication via Security Server
The Netop Security Server verifies the Guest identity by letting the Host relay the authentication process to a Windows Domain controller.

Directory Service Authentication via Security Server
The Netop Security Server verifies the Guest identity against a Directory Service via LDAP.

RSA SecurID with ‘Triple-factor authentication’ via Security Server
The Netop Security Server combines RSA SecurID ‘two-factor authentication’ with a shadow Netop Guest ID password.

Centralized 2 and 3 Factor Authentication (see above)
Netop can be set to terminated a session after a timeout period and be instructed to lock the computer automatically.
*See the table on the following page...

Netop Logging
Netop can record all sessions verbatim to document the entire remote session. Netop Security Server provides a central log with more than 100 events and stores this information in an ODBC-compliant database for maximum security and scalability. Log data can be kept for an unlimited time along with the physical support session providing complete audit and playback capabilities.
Smart Card Authentication and Tunneling

By using a Smart Card and a Smart Card reader at the Windows Guest, the Windows Host is now able to authenticate the identity of the Guest user via the Security Server that communicates with a Windows server with Microsoft CA installed. If the Host computer demands local logon using Smart Card the Guest user’s credentials will be tunneled to the Host in order to provide the information.

*See Table Below

Encryption

Data transmitted between Windows, Linux, Solaris and Mac OS X modules can be encrypted using the Advanced Encryption Standard (AES – FIPS 197) with key lengths up to 256-bits.

Integrity and Message Authentication

Verified using the Keyed-Hash Message Authentication Code HMAC SHA-1 (FIPS 198-1/FIPS 180-3) or HMAC SHA-256 (FIPS 198-1/FIPS 180-3) based on the Secure Hash Standards SHA-1 (FIPS 180-3) or SHA-256 (FIPS 180-3).

Key exchange

Encryption keys for encrypted data transmissions are exchanged using the Diffie-Hellman method (SP 800-56 A) with key lengths up to 2048 bits and up to 256-bit AES (FIPS 197) and up to 512-bit SHA HMAC (FIPS 198-1/FIPS 180-3) verification.

Algorithms used by Netop Remote Control

<table>
<thead>
<tr>
<th>TYPE</th>
<th>ALGORITHM</th>
<th>FIPS 140-2 APPROVED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key Exchange</td>
<td>Diffie-Hellman</td>
<td>Yes - SP 800-56 A</td>
</tr>
<tr>
<td>Symmetric Key</td>
<td>AES (Key sizes: 128-256)</td>
<td>Yes - FIPS 197</td>
</tr>
<tr>
<td>Digest</td>
<td>SHA-1</td>
<td>Yes - FIPS 180-3</td>
</tr>
<tr>
<td></td>
<td>SHA-256</td>
<td>Yes - FIPS 180-3</td>
</tr>
<tr>
<td></td>
<td>SHA-512</td>
<td>Yes - FIPS 180-3</td>
</tr>
<tr>
<td>Message Authentication Code</td>
<td>HMAC SHA-1</td>
<td>Yes - FIPS 198-1/FIPS 180-3</td>
</tr>
<tr>
<td></td>
<td>HMAC SHA-256</td>
<td>Yes - FIPS 198-1/FIPS 180-3</td>
</tr>
<tr>
<td></td>
<td>HMAC SHA-512</td>
<td>Yes - FIPS 198-1/FIPS 180-3</td>
</tr>
</tbody>
</table>