

# Security

Every system claims to be HIPAA-compliant, but to truly ensure the privacy of your data you must ensure that unauthorized users are kept out. Access to your ATS System is tightly controlled. Unlike systems that rely on the features built into the web browser for security, ours is accessed via a virtual private network (VPN). This enables us to provide a much higher level of security. Some of the advantages include:

### Encryption

When you connect to our network you create a secure “tunnel” between your system and our servers. All the data sent back and forth through this tunnel is encrypted so that it can only be unlocked when it is received at the other end.

### No Public Access

SSL encryption is the minimum you would expect from an online application but it still allows anyone access to a web site. A poorly programmed application might have a “back-door” that allows a savvy hacker to see client data. Our system provides two-stage authentication – first, users must be validated on our VPN. If they are not authenticated they are prevented from going further – they can’t even see the home page. Once validated, the user logs into the application. Each user has a unique identity and role on the system that determines what information they have access to. For example, only the person who writes a progress note can modify the contents of it.

### Host Checking

Before users can even reach the login page of our system, their system is examined to ensure it complies with security policies. We provide a robust Host Checker that checks for antivirus software, firewall software, spyware software and current operating system service packs. We can also tell it to check for certain programs or files on the computer that is connecting and grant/deny access based on what it discovered.

*“A site that merely provides data encryption has no protection against spyware and other malicious software.”*

The second part of host checking involves our Advanced Malware Protection. This scans a user’s computer for keyloggers, screen capture software, trojan horses, spyware, malware and other malicious software. This is particularly important because these applications work in the background to capture passwords and user identity. A site that merely provides data encryption has no protection against these threats. Our system does.

### Audit Trail

Any time data is changed in ATS our software makes a copy of the change in our audit system which includes what was changed, when and by whom. If data is modified it is easy to determine which person made the modification.

### End-To-End Security

Finally, when the user has completed their work and exits the system, the Cache Cleaner cleans out any information from their online session that may be stored in the computer’s memory. This prevents another user from going in after someone else and attempting to access client data using leftover session variables and query strings.