Online Data Protection

Info Sheet

V1.0
June 2010

Online Applications

Many healthcare organizations are choosing to capture the massive gains in efficiency, productivity, and cost savings through using the internet for business. Like all forms of business, the web brings with it unique challenges and risks that Ormed is aware of.

Please rest assured that we are taking every opportunity to safeguard your organization's data when you use our online applications.

How does Ormed protect my data?

We employ two primary strategies to protect client data.

1. All communication between the client browser and the server can be configured to use Secure Sockets Layer (SSL) or Transport Layer Security (TLS).

   This simple step ensures that any data being sent between the client and server is encrypted and **can not be viewed** using eavesdropping techniques such as packet sniffing. However, please note that each site running ORMED MIS software that exposes data **outside** of their firewall needs to purchase a signed certificate to ensure all communications are secure.

   If all applications are running in a secure intranet, then the certificate and transport security mechanisms are optional.

2. Web services are secured using token-based authentication. This means that when a user successfully logs in, they are issued a token.

   Each web service call uses that token to ensure non-authorized users do not have access to any data on the server. These tokens expire; if a user leaves their computer for an extended period of time they will need to login again, which adds additional security at the workstation level.