Topic	SOS Data Security
Document #	109
Product	ALL
Author	Seth Krieger
Last Revised	January 15, 2010

SOS Data Security

>> How is access to the clinical data controlled? I assume that there is a way to control access to files so that nobody except for the clinician or his/her supervisor (where applicable) could access the clinical files for a given patient? <<

Throughout the system, access to specific patients is controlled by the User Patient Lists in the Admin Module.

>> And related to this, are the data files encrypted? If so, what type of encryption algorithim is used? <<

By default, the database is not encrypted. Optionally the user may select simple encryption (obfuscation) when rebuilding the database. Strong database encryption is available (see Document #111), but a better approach is encryption of the disk partition on which the SOS system and database are stored (using a product like TrueCrypt or Microsoft's BitLocker). It is very likely that you have other sensitive information on your system, outside the SOS database. By encrypting the entire disk, the database and all stray information are equally protected. Disk encryption should *always* be used on computers that are transported from location to location.

In addition to encryption of the database itself, a customer might be concerned about protecting the data while it is in transit between the server and the client workstations. Various network protection approaches are available, including VPN, wireless encryption, and built-in Terminal Services encryption. There is an extra-cost option for the Sybase ASA database that provides very strong encryption of network packets for JUST SOS database traffic on the network, but the customer should consider more global approaches that protect all network communication, not just SOS data.