

4.3 Data Security for the PENS Computer

The available methodologies to protect the access for notebook computers are data encryption, signature verification, and voice verification.

Data encryption is the most common data security technology for controlling access to a computer. The most common data encryption technology for the PC is DES. The software, such as Assure from Cordant, Inc, provides authentication of users at the workstation level, selective audit of user activity, and protects information through a seamless combination of access permissions, as well as automatic encryption.

Signature verification is the way for specifically controlling access to a pen-based computer system. The Signature Verification for Windows from Sign-On Systems, Inc is an example of this type of software that can be integrated into the PENS software. First, it will create the signature template, which is an encoded version of all the signature data. The template can be stored in a file or database for later retrieval. The verification process consists of testing all the templates and returns the results. The pen-type device, which should install at all pen-based system, is recommended for signature verification.

Voice verification is another method for controlling access to a workstation. This concept is very similar to signature verification, except it uses a voice template instead of handwriting template for verification. The Voice Tools from Dragon Systems offers the software and hardware for this technology.

At this time it is our opinion based upon the research we have conducted that neither the voice nor handwriting recognition technologies are mature enough for implementation for the PENS program.