Computers and
Confidentiality

To an almost awesome degree, computers have become holders of a person's most sensitive and jealously guarded secrets. They possess delicate information on everything from military weapons systems to much sought after industrial formulae. And, increasingly, they are the vaults holding highly confidential medical records on millions of patients.

Protecting that information from "unauthorized eyes" is vital not only from an ethical point of view but because of the potentially explosive legal ramifications of unauthorized disclosure.

Patient confidentiality, the commandment of Hippocrates, is paramount, and where humans have chosen to place this onus on inanimate electronic computers, a parallel responsibility emerges – its security. As with any computer network, however, certain people must have access to specific information in the course of caring for patients.

Isolation Systems Limited, has developed "Enigma", a data protection storage system to guard sensitive information while not making the process so complex as to discourage its use.

Where only mainframe computers once stored and provided data, personal computers (PCs) operating as remote or portable terminals are now doing the same thing through the use of hard disks to which access is often easier. While hard disks, or diskettes, can be locked in vaults, this is not always done. Further, while efforts have been made to classify certain information as sensitive or confidential, problems occur when, for easier access, some institutions classify such information as being of a "general" category. Such a rating may, in the process, ignore adequate protection of data.

The Enigma incorporates a key management system which, according to the manufacturer, provides a rapid, easy way of using an encryption or ciphering facility to protect stored data on either hard disk or diskette.

The facility can encrypt a 1 000-byte file in 0.6 seconds using a diskette drive. On hard disk it is even faster. The user has a choice of either encrypting a file under a unique "self-nominated" key or a "default" key assigned to the particular PC station. A file encrypted under a user-nominated key can only be accessed by that user since the same key is needed for decryption. This technique permits transportation of encrypted diskettes which can then be decrypted at the end destination.

An alternative feature permits a security officer to designate a default key for all authorized individuals using a particular station, which allows them to encrypt or decrypt files without their having to know the key. Because the user does not know tne encryption key, the file can only be decrypted at the same station, thereby making it non-portable.

Each station in an Enigma system permits up to eight authorized users who use a log-on identification and password; users can change their passwords at each log-on.

An anti-tampering feature provides an automatic response ranging from invalidation of a password to complete shutdown. A log is created on all tampering violations for later analysis.

Isolation Systems also manufactures a range of systems including a line isolation monitor for detection of electrical leakages in critical hospital areas.