

Working Group on Confidentiality and Information Systems in GU Medicine Clinics and Sexual Health Clinics where patients seek care or advice for STDs.

No information system, whether manual or computer based is totally secure. There are steps that can be taken, however, to increase security to a level that is satisfactory. The decision of every information system owner is the length to which they want to go to achieve a satisfactory level of security. Whilst some steps do not have costs associated with them, the majority will have, and this reduces the issue of security to cost benefit analysis. The ultimate responsibility of the system remains with the information system owner, whether this be a Consultant, Business Manager or IT department and the issue of responsibility should be clearly identified and understood by all parties involved. No clinic should be forced into arrangements they are unhappy with or that they feel compromise confidentiality.

Storage/Physical Security

Security Marking

Engraving or etching all pieces of equipment will make it unattractive to thieves to steal the equipment.

Chaining

Chaining equipment to fixed points will make it more difficult to steal. In response to this a number of thieves are smashing CPUs and only taking the chips. It is possible to case the CPU in steel units but this is costly. Restricting access to the CPUs is on a unit basis more cost effective. It is particularly important that the fileserver unit is situated securely, well ventilated, with limited access.

Burglar alarms

Restricting access to the clinic when nobody is present and a direct link to security means that unauthorised access can be limited to a few minutes. This will help to protect manual and computerised information systems. There are some problems to do with necessary access that need to be considered eg cleaning staff and deliveries. Maintenance of security and limiting access will need careful consideration if the clinic areas are also used by other services.

Locking office doors/filing cabinets

Where possible doors should be locked when not in use to deter possible breaches in security. This applies to both manual and computerised information systems.

Recording all serial numbers etc.

If a theft occurs then a register of serial number which can be provided to police is a useful measure and increases the chances of recovering stolen property.

Encryption

Data should be stored in an encrypted form. This will make it more difficult to access data, should a breach of security arise. There are a variety of different packages which vary in price and ease in which to break, the decision again falls to the information system owner. Data transmitted to outside information systems should also be encrypted during transport.

Processing

Passwords

Access to the system should be restricted by passwords. These should be given to authorised personnel and changed on a regular basis. It is advisable to change passwords on at least a weekly basis. They should not become public knowledge, be written down, shouted out or be too obvious e.g. family names/football teams etc. Individual passwords are more advisable than group ones.

Access rights

Different users require access to the system. Users should not be able to access data they do not require. By using the identity of the users, rights can be assigned which dictate the usage of the system.

No external disk drives on PCs

This will prevent the possibility of downloading data/ programmes onto removable disks. It will also prevent the unauthorised use of foreign software and reduce the risk of virus infection. Locks are available which prevent unauthorised use of a disk drive if drives are required.

Location of screens

Screens should be located in positions which limit anyone other than the user seeing the screen. If this is not possible then consideration should be given to what is displayed on these screens and password protected screen savers used when not in use.

Data Validation/verification

The integrity of the data is vital for the survival of the system. Information entered needs to be verified/validated and the results of processes confirmed as correct.

Audit

An audit log of events is important to identify who has changed what information on the system. This can be achieved by the software keeping an automatic log of certain events and the login identity of the user making the changes.

Automatic log out.

Terminals that have not been used for a given period of time should log out of the system automatically.

Communications with other Information Systems

Local Area Network (LAN) v Hospital Network

PCs once networked pose a problem in that the access to data is not restricted to the PC on which the data is stored but extended to all PCs connected on the network. All of these PCs have to be made as secure as possible. The advantage of a LAN, where there are no connected PCs outside the department, is that the whole issue of security is then the responsibility of the Department and access to the department is required to gain access to a terminal. If the information system is part of the Hospital network then any terminal on the network has the potential for access to the data and the security of the system relies on steps taken by the owners of the Hospital network rather than the department. The main advantage of a Hospital network is the ability to share information. Due to the confidentiality surrounding GU Medicine clinics this is not possible or desirable. Therefore Local Area Networks are recommended. Any connection outside the department should be perceived as a potential breach of confidentiality and security. It may be desirable to transfer some information between the GUM network and the Hospital network - see linking with labs. If a clinic has no other option than to be on an hospital network (not recommended) then the issues of responsibility must be clearly established and documented. The security procedures of the Hospital network should be investigated and if necessary additional measures demanded. The ultimate decision lies with the clinic but responsibility for security on a Hospital network must lie with the managers of the network.

Networks

All the security features provided by networking software should be implemented. This includes but is not restricted to limiting users by time and station ID. Automatic network log detailing attempted log on attempts etc.

When logging, users other than the system supervisor, should only have access to the software/data they require, and on logging out should not have access to the operating system or other functions.

Modems

Modems pose a potential security risk by allowing access to the information system from outside the clinic. They use public phone lines which are not secure and there is an element of uncertainty as to who is accessing the system. The modem should not be left connected to the system all the time, but only (i.e. the person calls in and the system calls them back on a recognised number only). Whilst connected to the system a supervisor watches the access on the screen connected to the modem to ensure that programme files only are accessed and can disconnect if there is a potential breach in security. If used in this way, then there should be no more of a risk than other contractors in the department and the potential for access to manual files.

Remote/satellite clinic access

If the clinic is to be managed over a wide area then a LAN may not be possible. Encryption is a possibility or a tied line between sites. The decision on the steps to maintain security and confidentiality lies with the information system owner.

Linking with labs etc.

Great benefit can be obtained from sending electronic information to and from labs etc. This can be done in a variety of ways e.g. encrypted on disk, PCs polling encrypted data across networks etc. Any direct link has the potential to be violated and must be considered when evaluating the security of a system. Data received from external sources should be checked for viruses, either on a stand alone PC or using more comprehensive FileSaver based virus checking software.

External request for information

The identity of a requester must be established and the use to which information will be put before any information is released. The permission of the information system owner must be sought for the release of any information. Compliance with the Data Protection Act as well as the Acts and regulation governing GU Medicine must be maintained.

Survival of the System

Security needs to include the ability of the system to survive disaster situations and plan to prevent the system becoming obsolete.

Disaster recovery

Is the ability of current procedures to minimise the down time of any system in the event of a disaster, whether from a threat to security e.g. intruder/theft, or from fire/hard ward fault, or to prevent a disaster occurring. Again as with the general issue of security the steps that can be taken are almost limitless with cost/benefit being the decision of the information system owner. There are companies which specialise in disaster recovery who can hold a copy of the system for you which you utilise only in the event of a disaster. The nature of the information held makes this option unrealistic, but there are a number of procedures that can be implemented within departments to reduce the impact of a disaster situation.

Backups

A comprehensive procedure whereby regular backups are made of the data is vital. This will guard against the system not being able to withstand a disaster situation. There are many different ways of backing up data the most common being a tape stream backup. This will allow the entire system to be reinstalled if for any reason there is a problem with the working copy. Decisions need to be made as to how often to make backups. It is advisable to backup any files that have been changed on a daily basis (this will mainly be data files) and the entire system on a weekly basis. It is important that the backups are done when the system is not in use and all users are logged off the network. Ideally backups can be automated in an overnight process. It is also important to use several tapes in rotation so that a problem with one tape will mean that there is a recent backup to the failed tape. A minimum of 6 tapes should be used. One for every day of the week and one for the system backup. Backup tapes should be checked to ensure that recovery is possible from the tapes on a regular basis. Tapes should be stored so that any damage to the system e.g. Fire, will not affect the tapes. The best option to maintain security and limit access is a fireproof safe kept onsite.

Removable hard disks are an option for smaller systems. They should be locked in a fireproof safe and backups still made in case of hardware failure.

Information may require either to streamline the system or whilst the system is inactive. Other technology exists for the longer term backup of information including optical disks/CD roms. The security and possible access to these should be considered before implementation.

Fireproof safes

Provide secure storage which can withstand a fire if necessary whilst still protecting data. They are ideal for storing tape backups and original software disks. If backup tapes are not kept on site, then careful consideration should be given to their security and the possible access to them.

Storage on hard disks

Theft of computer equipment tends to be for the equipment itself rather than information stored on it. This being the case patient identifying information should not be stored on any hard disc other than the Filesaver (which should be encrypted and chained and locked away). If this is not possible then it should be encrypted and password protected.

Anti-virus

Viruses are rogue programmes that are designed to corrupt information or other programmes. There are anti-virus programmes which can be used to detect and cure viruses. These should be used on a regular basis to check all machines and be installed permanently on a Filesaver.

Support/Maintenance Contracts

Support and maintenance contracts are important for the long-term survival of the system and allow for faults to be rectified. It is advisable to cost these in to the future at the time of purchasing a system in order to place a true cost on different systems.

Any work done on the system by outside support staff should be done on a copy of the programme using dummy data so that the actual data files are not used. In this way changes can be made without access to the real data. This applies whether the staff are on site or access is via the modem. Information owners must be completely satisfied as to observance of confidentiality requirements by support companies. If necessary Support companies can be required to sign confidentiality agreements with financial penalties and termination of contract clauses if they do not perform to standard.

New versions of software

For the long term survival of any information system, periodic reviews should be carried out to see if the current system, whether manual or computerised, is still reaching its objectives. If not then steps should be taken to update the system to meet the changes in requirements.

Other Issues

Fax machines

Use unsecured telephone lines with little knowledge about the security and confidentiality at the receiving end. The transmission itself is unsecured and susceptible to interception by third parties. Unlike modems the transmission itself is not routinely encrypted. This should be considered before transmitting patient identifying information. GMC has extended its guidelines to cover the transmission of information electronically by computer or fax. See Professional Conduct and Discipline: Fitness to Practise - paragraph 78. This places the responsibility onto the Doctor to be satisfied that the transmission is secure.

Telephone Calls

Security and confidentiality needs to be considered not only in terms of who is being spoken to (there is no certainty regarding identity) but also who can overhear conversations within the department. The telephone lines are unsecured, unencrypted and susceptible to interception. Messages left on answer phones can be replayed by anybody with access to the answerphone.

Post

Patient identifying information is routinely send through the post with little consideration given to its security or the potential for breaches in confidentiality. This should be considered when reviewing the subject within a GU department.

Data Protection Act

Compliance with the DPA is required by any computerised information system.

Manual Files location

Security and confidentiality needs to be considered as much for manual files as computer based information. This includes their location e.g. locked filing cabinets, usage e.g. lying around the clinic, and transportation e.g. to satellite clinics. Other issues outlined in this document e.g. validating information and auditing who writes in the notes also apply to manual notes.

Old Equipment

Before old equipment is disposed of it should be removed of all information. This should include reformatting all disks as deleting information is not sufficient. It is also important to ensure that all disks that are removed from the clinic have never had any confidential information on them, even if it has been deleted. If this is the case then these should be reformatted as well.