Chapter 3 – Deliberate tampering Patient record systems – purposes and characteristics

3. *Deliberate tampering Patient record systems – purposes and characteristics*

This chapter sets out the purposes and characteristics of patient record systems. These requirements underline existing good practice about the use of national, standard approaches. Integrated systems, with appropriate arrangements for sharing information, place even greater emphasis on the need for:

- Consistent standards through the use of the patient CHI Number (NHS Number in England) and agreed national coding schemes
- Excellent data quality.

3.1 Clinical purposes

General practices require a patient record system that has the following functionality;

- Facilitate the clinical care of individual patients by;

1 Assisting the clinician to structure his or her thoughts and make appropriate decisions

2 Acting as an aide memoir for the clinician during subsequent consultations

3 Making information available to others with access to the same record system who are involved in the care of the same patient

4 Providing information for inclusion in other documents (e.g. laboratory requests, referrals and medical reports)

5 Storing information received from other parties or organisations (e.g. laboratory results and letters from specialists)

6 Transfer the record to any NHS practice with which the patient subsequently registers

7 Providing information to patients about their health and health care

- Assist in the clinical care of the practice population by;

8 Assessing the health needs of the practice population

9 Identifying target groups and enabling call and recall programmes

10 Monitoring the progress of health promotion initiatives

11 Providing patients with an opportunity to contribute to their records

12 Supporting medical audit

3.2 Non-clinical purposes

Practices also need a patient record system that can be used to meet administrative, legal and contractual obligations by;

- Providing medico-legal evidence (e.g. to defend against claims of negligence)

- Providing legal evidence in respect of claims by a patient against a third party (e.g. for injuries, occupational diseases and in respect of product liability)
- Meeting the requirements of specific legislation on subject access to personal data and medical records
- Recording the preferences of patients in respect of access to and disclosure of information they have provided in confidence
- Providing evidence of workload within a practice or a PCO
- Providing evidence of workload to PCOs (e.g. to support claims and bids for resources)
- To enable commissioning of community and secondary healthcare services
- Monitoring the use of external resource usage (e.g. prescribing, laboratory requests and referrals)
- Assist with the completion and monitoring of certificates and reports for social, paramedical, legal and private purposes.

3.3 Additional purposes

Practices are increasingly likely to require a patient record system that can be used;

- To interact with a decision support/expert-system;
- To support teaching and continuing medical education.
- To support clinical governance activities
- To support professional appraisal and revalidation
- To enable;

13 Epidemiological monitoring

14 Surveillance of possible adverse effects of drugs

15 Clinical research

3.4 Electronic and paper records - characteristics

Most of the purposes described above are generic, applying equally to both paper-based and electronic patient records. However, electronic and paper based record systems do differ in several crucial characteristics. These are listed below;

3.4.1 General characteristics

3.4.1.1Physical

EPRs depend for their existence on the presence of supporting hardware and software. In so far as EPRs have a physical presence, this exists at the point(s) of data storage on the machine(s), involved, though they may be accessed remotely. Paper records exist only where they are physically located (or copied).

3.4.1.2Accessibility

EPRs may be available to the clinician at any point where electronic access is provided to the recorded data. Paper records have to be physically present at the point of use.

3.4.1.3Resource

Paper records are generally cheap, EPRs are expensive. EPRs require investment in the necessary hardware, software, maintenance, upgrades and training. This may be offset against savings in other costs for the paper equivalents but there remains a different order of investment type and magnitude for computerised records.

3.4.1.4Predictability

Paper records are generally predictable in their form and function. This is not necessarily the case for EPRs where the user interface, system architecture and functionality may vary considerably between suppliers. This has major implications for training, support and transfer of clinical information between systems (see chapter 5 of these guidelines).

3.4.1.5Maintenance

Paper records require little maintenance beyond filing and internal ordering. EPRs have additional requirements in terms of technical maintenance, upgrades, and preservation of their integrity, which require quite different organisational skills and resources.

3.4.1.6Training

Paper records are generally regarded as intuitive in their use. Although clinicians may receive some training in aspects of record construction, this is mostly to do with their semantic content rather than the specifics of the interaction between themselves and their records. Most EPRs are not usable without both basic IT skills and system specific training.

3.4.2 Record characteristics

3.4.2.1Data entry

Data entry in paper records is relatively straightforward and usually consists of unstructured or semi-structured narrative, abbreviations and perhaps a diagram. The notes may make reference to other parts of the record and may be problem-orientated or summarised. Data entry into the EPR usually contains narrative and structured (coded) entries, together with attached files such as documents and images linked to specific records. Coded data entries can be searched quickly by computers and EPRs can present users with different information based on their level of access and the task in hand

Care must be taken to ensure that patients and records are correctly matched so that data entered into the EPR is for the correct patient.

3.4.2.2Data retrieval

Data retrieval from EPRs is easier than from paper - not just because EPRs are physically more accessible to their users than paper records - but also because the ability to interrogate the content of EPRs for audit and analysis purposes is arguably their single greatest advantage over their paper equivalent.

3.4.2.3Semantics

Paper records generally depend for their meaning on the intention and semantic competence of their author(s). There may be some additional organisational elements that affect semantics (such as the way the paper is ordered, the presence or absence of a meaningful summary etc.) but the crucial aspect of the paper record is that it provides considerable freedom of expression for its authors in communicating their meaning. EPRs, on the other hand, always constrain to a greater or lesser degree what is possible to be entered into them. However, a properly constructed EPR with narrative and clinical codes is less ambiguous than a paper record with abbreviations and personal shorthand. The design of EPRs in terms of the availability of coded information and the relationship between those codes and text entry as well as other elements of structure such as problem orientation, access to documents and the like requires particular semantic skills for good usage. This, in turn, contributes to the training requirement.

Furthermore, while electronic records carry advantages over paper ones in terms of processability (e.g. audit, automated decision support, warning of alerts etc.); the corollary of this is that in EPRs there is a "machine" element to the semantic which is not present in the paper record. In other words, computerised records will only give added value if they are provided with data in predictable ways. This is commonly paraphrased to "garbage in garbage out". This fact carries an additional training implication and may be crucially important in terms both of reliable organisational decision-making based on computerised information and, more importantly, for safe patient care.

Common standards across the professions for electronic patient records are a requirement for consistent high quality clinical records. In England, the Information Standards Board (ISB) has launched the NHS Health Record and Communication Practice Standards for Team-based Care - a standard which ensures that NHS staff from different healthcare professions record and communicate patient information consistently . Whilst useful as guidance, there is no formal equivalent organisation in Scotland and health care professionals in Scotland must continue to rely on individual guidance issued by their own professional body.

It is important to understand that transferring electronic patient data is not the same as transferring meaning and context.

3.4.3 Legal characteristics

For the most part the principles of behaviour that underpin legal and professional aspects of medical record keeping are similar for paper records and EPRs, there are significant differences in the effects of the law on principles of good practice for computerised records compared to paper records;

3.4.3.1Medical confidentiality

There is no UK statute law that expressly asserts the obligations, commonly referred to as medical confidentiality. Information held in confidence is protected legally by common law, the Data Protection Act 1998 and professionally by the GMC.

3.4.3.2Access to records

Access to electronic and paper records are covered by the Data Protection Act (DPA) 1998.

3.4.4 Security characteristics

There are several aspects of security that particularly relate to electronic records. Within this document, we use the elements of computer security as defined in the Open Systems Interconnection Model (of the International Standards Organisation). The baseline security standard for the NHS is BS7799. Aspects of security that need particular consideration in relation to electronic records are;

3.4.4.1Availability

This refers to the extent to which a record is accessible and useable upon demand by an authorised entity.
Paper records are available if they are physically present. The availability of EPRs is more complex and does not depend upon their physical location, and they are more difficult to lose, destroy or alter.

3.4.4.2Integrity

It is important that the data as stored cannot be altered or destroyed in an unauthorised manner either by deliberate intent or through errors in the computer software.
There are specific requirements for EPRs to ensure their integrity, including an audit trail of data entry and modification in addition to the physical security of the record.

3.4.4.3Accountability

Any entity (whether machine or person) which is able to create, read, edit or delete from the record should be identifiable both from and to their activities.
For a paper record this amounts to a signature. In EPRs, this includes access logs, authentication and audit trails.

3.4.4.4Confidentiality

The property that information is not made available or disclosed to unauthorised individuals, entities or processes.
Medical confidentiality should not be compromised by the type of record system used. This means that EPR systems should include access control measures, physical security and privacy of systems and secure communication between systems.
The legal and security characteristics of EPRs are considered in greater depth in Chapter 3 of these guidelines.

3.5 Information Governance

3.5.1 Definition

Information Governance provides a framework for handling personal information in a confidential and secure manner to appropriate ethical and quality standards in a modern health service. There are a number of tensions (such as the need to balance the requirement for communication between clinicians against a patient's right to confidentiality) which render this a complex area, but it is not an area that clinicians can afford to neglect.
Information quality, whilst a key element of information governance, is particularly important in the context of these guidelines and is considered separately in chapter 4.

3.5.2 Rationale

NHS organisations in general and primary care teams in particular are increasingly expected to work in close collaboration with other organisations both within and without the NHS family. It is expected that NHS organisations will endeavour to ensure that services delivered are appropriate to the needs of patients and of high quality. This implies that NHS organisations and other involved bodies should communicate all relevant information between themselves in order to ensure that services delivered are both consistent and fully compatible with patient needs. However, the delivery of services to patients must remain within the legal, ethical and policy framework. This framework needs to be understood by all involved in sharing patient information.

3.5.3 Scope

Information governance encompasses the principles that apply to the processing and protection of information in whatever form it is processed and utilised. Inclusion of this topic in these guidelines should not obscure the fact that these principles apply equally to written records, oral communications and other media e.g. photographs and x-rays.

3.6 Legal aspects

Important elements of information governance for NHS bodies are derived from legislation and common law. Some of these elements are clear-cut but many others need interpretation. NHS service delivery requirements, an understanding of acceptable ethical practice and applicable SEHD policy and standards will all impact on this interpretation. The relevant areas of law are listed below, with an indication of the implications of each.

3.6.1 Common law duty of confidence

The common law in Scotland is based on precedent. As a result its impact is not always clear and it may change over time. Whilst various interpretations of the common law may be possible, there is widespread acceptance that it reinforces the need to obtain consent from patients before sharing information about them. This duty is not absolute and there are a range of bodies, such as the courts and NHS Boards that have statutory powers to require disclosure of information.

3.6.1.1Key attributes

Confidential patient information may only be disclosed:

- with a patient's consent, or
- where it is required or permitted by law (statutory instrument or Court Order), or
- where the public good achieved by disclosure outweighs the individual's right to confidentiality.

3.6.1.2Key guidance

- Confidentiality: NHS Scotland Code of Practice
  http://www.confidentiality.scot.nhs.uk/publications/6074NHSCode.pdf
- GMC Confidentiality: protecting and providing information
  http://www.gmc-uk.org/guidance/library/confidentiality.asp
- SEHD confidentiality website
  http://www.show.scot.nhs.uk/confidentiality

3.6.2 Computer Misuse Act 1990

The Computer Misuse Act identifies a range of offences relating to unauthorised access to or unauthorised modification of computer records. It may apply where an unauthorised third party accesses information being transferred. Enforcement is difficult and prosecutions uncommon under this Act.

3.6.2.1Key attributes

Where systems are used other than by authorised staff for approved purposes it is likely to be a criminal offence.

3.6.2.2Key guidance

- Computer Misuse Act 1990
  http://www.opsi.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm

3.6.3 Access to Health Records Act 1990

The Access to Health Records Act provides a qualified right of access to the health record of a deceased individual where the person seeking access has an interest in the estate of the deceased. It only applies to records created after 1st November 1991.

3.6.3.1Key attributes

Permits those with an interest in the estate of a deceased individual to have access to that individual's health record unless the individual concerned has provided advance notification that they don't want this to occur.

3.6.3.2Key guidance

- Access to Health Records Act 1990
  http://www.opsi.gov.uk/acts/acts1990/Ukpga_19900023_en_2.htm
- Scottish Executive Health Department
  http://www.confidentiality.scot.nhs.uk/access_medical_records.htm

- Dept of Health, patient confidentiality and access to health records http://www.dh.gov.uk/PolicyAndGuidance/InformationPolicy/PatientConfidentialityAndCaldicottGuardians/fs/en
- BMA Ethical Committee - Access to Health records by Patients (Dec 2002) http://www.bma.org.uk/ap.nsf/Content/accesshealthrecords

3.6.4 Data Protection Act 1998

The Data Protection Act sets out eight principles which define the conditions under which processing (including recording, storage, manipulation and transmission) of personal data can be determined to be legally acceptable or otherwise. The act also identifies the sensitive nature of health information and particular needs of health professionals to communicate that information between themselves. The Act gives patients rights of access to their medical records and applies to electronic and paper-based record systems. The eight principles are listed below:

1 Fairly and lawfully processed
2 Processed for limited purposes
3 Adequate, relevant and not excessive
4 Accurate
5 Not kept for longer than is necessary
6 Processed in line with subjects' rights
7 Secure
8 Not transferred to countries without adequate protection

3.6.4.1Key attributes

The Act requires that patients are told about who will see their personal data and for what purposes. It does not prevent clinical data being used for NHS purposes but other uses may require explicit patient consent. N.B. the common law requirement for consent applies to all uses of confidential patient information.

3.6.4.2Key guidance

- Data Protection Act 1998 http://www.hmso.gov.uk/acts/acts1998/19980029.htm
- Data Protection Act 1998: Legal Guidance http://www.ico.gov.uk/
- UK Information Commissioners Office http://www.ico.gov.uk/
- Use and Disclosure of Health Data http://www.ico.gov.uk/documentUploads/Use%20and%20Disclosure%20of%20Health%20Data.pdf
- Health Rights Information Scotland – How to see your Health Records http://www.scotconsumer.org.uk/hris/leaflets/athr/index.htm

3.6.4 Human Rights Act 1998

The Human Rights Act is based on the European Convention of Human Rights. The act identifies 15 human rights in Schedule 1 and requires 'public authorities' to ensure that their activities do not violate these rights. Individual doctors working within the NHS are almost certainly public authorities under the HRA and are therefore required to observe the Convention rights in their decision making, and demonstrate that they have done so.

3.6.5.1Key attributes

The Act provides a right to respect for privacy (article 8) that can only be set aside in accordance with the law when considered necessary in a democratic state. The advice from Government is that this right is respected fully where the requirements of the Data Protection Act 1998 and the Common Law duty of confidence are complied with.

3.6.5.2Key guidance

- Human Rights Act
  http://www.hmso.gov.uk/acts/acts1998/19980042.htm

3.6.6 Freedom of Information Act (Scotland) 2002

The Freedom of Information Act gives a general right of public access to all types of recorded information held by public authorities (including GP Practices), sets out exemptions from that general right, and places a number of obligations on public authorities.

3.6.6.1Key attributes

Whilst there are a number of exemptions, the main one that will apply in a primary care setting relates to confidential patient information. Requests have to be dealt with within 20 working days.

3.6.6.2Key guidance

- FOI Scotland 2002
  http://www.opsi.gov.uk/legislation/scotland/acts2002/20020013.htm
- Scottish Information Commissioner
  http://www.itspublicknowledge.info/

3.6.7 Electronic Communications Act 2000

This Act sets in place an approval scheme for businesses providing cryptography services, such as electronic signatures and confidentiality services, and the processes under which electronic signatures are generated, communicated or verified. An NHS order made under the Act allows for the creation and transmission of prescriptions by electronic means in cases where specified conditions are met.

3.6.7.1Key attributes

An NHS order made under the Act allows for the creation and transmission of prescriptions by electronic means in cases where specified conditions are met.

3.6.7.2Key guidance

- Electronic Communications Act 2000
  http://www.hmso.gov.uk/acts/acts2000/2000007.htm

3.6.8 The NHS (General Medical Services Contracts) Regulations 200411, the NHS (Personal Medical Services Agreements) Regulations 200412 and the APMS Directions

These Regulations, which came into force in support of the new GP contract, include provisions relating to patient records, the confidentiality of personal data, rights of access to, and the provision of patient and practice information held by contractors.

3.6.8.1Key attributes

The Regulations provide NHS Boards with the power to require patient, and other, information to be provided by practices where this is necessary in order for them to discharge their responsibilities. These Regulations override common law confidentiality but the use of these powers must be governed by a Code of Practice.

3.6.8.2Key guidance

A Code of Practice is currently being drawn up by the Department of Health in consultation with the GPC. This Code aims to ensure that the powers are invoked only where strictly necessary and that anonymised data is used wherever practicable.

3.7 Standards

In addition to the requirements of law, there are a range of standards that contribute to the information governance framework.

3.7.1 ISO17799:2000 and BS7799-2:2002 Information Security Standards

BS7799-2:2002 is a British standard, and BS7799-1 has been adopted internationally as ISO17799:2000, which expresses a code of practice for information security management. It is the standard adopted by the NHS for information security management.

3.7.1.1Key attributes

Information security needs to be based upon an assessment of risk and covers issues such as access controls, physical security (doors and locks etc), business continuity planning and disaster recovery, capacity management, and the storage and disposal of records

3.7.1.2Key guidance

- British Standards Institute
  http://www.bsi-global.com/index.xalter
- NHS Scotland IT Security Policy and Manual
  http://www.security.scot.nhs.uk/

3.8 Other relevant publications

3.8.1 Caldicott Report 1997

The Caldicott review was commissioned to examine the ways in which the NHS used information. The report lists 6 principles to apply to indicate the appropriateness of a proposed communication. The report also carries 16 recommendations for changes in communication processes and practices employed by the NHS. The recommendations focus on the adoption of a strict 'need to know' approach to the transmission of identifiable information and the establishment of an educational and supervisory framework to ensure its implementation. Although much of the work recommended by the Caldicott Committee has been superseded by the NHS Information Governance initiative, the underlying Caldicott principles and the requirement for senior clinical involvement in confidentiality management remain highly relevant.

3.8.2 Confidentiality: NHS Code of Practice2

The NHS Code of Practice on Protecting Patient Confidentiality was published in August 2003 by the Scottish Executive Health Department. All NHS Scotland staff are contractually obliged to adhere to it.
The Code of Practice sets out individual and organisational responsibilities in a clear and coherent way, covering both confidentiality and aspects of the Data Protection Act 1998.

3.8.3 Medical Ethics Today: The BMA's handbook of ethics and law

The second edition of this book, published in 2004, provides in depth consideration of a range of information governance (and many other) issues where interpretation and judgement is called for.

3.8.4 Protecting Patient Confidentiality: Confidentiality and Security Advisory Group for Scotland (CSAGS)

This Report to Scottish Ministers was prepared by the Confidentiality and Security Advisory Group for Scotland (CSAGS). CSAGS was set up in September 2000 as an independent committee, supported by the Scottish Executive Health Department (SEHD), 'to provide advice on the confidentiality and security of health related information to the Scottish Executive, the public and health care professionals'.

3.9 Key information governance issues and developments

3.9.1 Informed consent

Other than when there is a clear legal basis for overriding confidentiality or, exceptionally, when the public good that would be served by breaching confidentiality is sufficiently great, the basis for use and disclosure of confidential patient information must be informed consent. A patient's consent can be implied (from their actions) or expressed (e.g. verbally or in writing) but must be based upon information and awareness that there is a choice.
The policy position established by the Department of Health, endorsed by the BMA, GMC and Office of the Information Commissioner, is that where the information sharing needed to support the care process and to assure the quality of that care has been explained to a patient and he/she has been offered the choice of refusing to

permit this, then consent can be implied. In other circumstances, specific and expressed consent must be sought.
Health professionals must take particular care not to disclose information about any third parties when they share or disclose health information without the specific informed consent of any such third parties. An electronic record of any such disclosures must be kept and linked to the originating record.
Detailed consideration of consent issues, including those relating to children and those who lack capacity, can be found in Confidentiality: NHS Code of Practice and Medical Ethics Today. With the bulk of patient contacts taking place within primary care settings, the effective informing of patients is a key primary care responsibility.

3.9.2 Anonymisation and pseudonymisation

Data that cannot identify an individual patient either directly or through linkage with other data available to a user does not need to be regarded as confidential. Whilst there may remain ethical and policy restrictions on the use of anonymised data, e.g. the requirement for all research to have ethics committee approval, the use of such data will not breach confidentiality or other legal requirements.
There are two categories of anonymisation:

1. Anonymised (unlinked) information has been stripped of any elements that would allow identification of individual patients.
2. Pseudonymised (linked) information has had any element that could lead to the identification of a patient removed (including the NHS or CHI number) but individual records are tagged with a reference or pseudonym which is unique for each patient and allows linkage back to the original patient data. An important aspect of pseudonymisation is that no one can access the lookup table apart from the originator who has a responsibility not to give anyone else access to this table. Where those who are using data have no means to reverse the process, and so no way to identify an individual from the data they have (or from the data they have and any they may acquire), the data may be treated as anonymised and there is no common law requirement to seek consent for their use. Processing should still meet at least one of the requirements in each of Schedules 2 and 3 of the Data Protection Act, however, since it is possible that pseudonymised data fall within the Act's definition of personal data. This point has not been tested in court, although the Information Commissioner advises NHS bodies and clinicians to apply the Act in these circumstances. For those who have access to both pseudonymised data and the means to reconstitute them, on the other hand, they should be treated as identifiable.

As a general rule, for purposes other than direct care or the quality assurance of that care it is advisable to work to the principle that:

1. wherever possible anonymised information will be employed,
2. that the use of pseudonymised information will only be considered where anonymised information cannot satisfy requirements, and that
3. patient identifiable information will only be made available where neither of the other categories can provide what is needed and it is lawful to do so.

3.9.3 Data ownership and control

GPs act as data controllers with their patients the data subjects. Debates about 'who owns the data' occur when a party wants to gain access to information held in patient records and there is uncertainty or disagreement about what category of information should be provided, whether the enquirer has any right of access, whether patient safety and/or privacy is at risk, or whether patient consent is required. It is generally more important to resolve these issues than the question of ownership as such and important to remember that "ownership" does not give rights of access or control to personal data.

3.9.4 Research

No disclosure of data should be allowed without the approval of the relevant patients, clinicians and research ethical committee(s). There may be legitimate reasons for extracting patient identifiable data from a GP system, other than for routine clinical care. However, such extraction should;

- Be with the knowledge and informed consent of the guardian of the record (in this case the GP)
- Follow approval from a Research Ethics Committee
- Follow approval from the responsible PCO
- And it should be with the informed consent of the patient

There should be both an audit trail for the data extraction and retention of the research database in order for both patients and health professionals to satisfy themselves, if necessary, that the data have been handled ethically and legally.
Provided both the patient and the practice have given informed consent, the ethics committee and PCO have approved and the data are handled according to the strictures of research governance, then the process should gain professional and public approval. However, researchers extracting these data would be well advised to;

- Inform a professional and public body and, if appropriate, seek endorsement from that body
- Only handle the data through a Trusted Third Party (TTP)

A Professional and Public Body could be a single body, or one could be set up for specific projects extracting data from general practice computer systems. Such a body should;

- Represent firstly the interests of patients and secondly the interests of the health professionals and practices
- Include independent lay people
- Include independent representatives of the medical, nursing and other relevant health professions in primary care
- Have full access if requested to the (anonymised) dataset, the extraction and use audit trail and the resulting analyses if necessary to satisfy themselves that the data are being used ethically and properly
- Have full access to agreements concerning the use of the data

- Be bound by rules and standards of patient confidentiality and data quality within the law

A TTP is an organisation or institution of reputation, that is independent of the SEHD, the National Health Service or commercial ownership or control, and that uses its reputation as a guarantee of the security and processing of the data. The essence of such a body is that it earns and maintains the confidence and trust of the public, the health professions and stakeholder organisations through integrity, transparency and equity. In future NHS Trust Service Providers (TSPs) may assist with the provision of "trust" services such as anonymisation and pseudonymisation.

3.10 Electronic communication and information governance

3.10.1 Clinical messaging

The scope of clinical messaging is planned to extend significantly. Plans include:

- Facilities to request and receive reports for the full range of laboratory and diagnostic imaging procedures;
- To receive notifications of hospital admission, of casualty and of OOH attendance;
- Electronic transfer of prescriptions from GP practices to pharmacies
- GP to GP electronic transfer of records

3.10.2 NHS e-mail "Contact"

The current version of NHS email provided by Cable and Wireless, known as "Contact", provides security for messages sent between two Contact email addresses. Contact email addresses can be identified by the suffix '@nhs.net'. Patient identifiable information can be safely sent from one Contact email address to another. If either the sending or receiving address is not a Contact address then separate encryption will be needed for sending confidential information including Patient Identifiable Data.

3.11 Other systems issues

PCOs rather than practices are now responsible for practice system purchase, maintenance, upgrades, support and training. Systems and suppliers will be accredited against National Templates and Service Level Agreements. Practices may not need to be so concerned in future with hardware issues, but the following headings still need to be considered;

3.11.1 Risk management

Practices should get help and advice about this from their PCO and National User Group.

3.11.2 Accessibility

Practices need to ensure that they have an adequate number of workstations at each point within the organisation where staff need to have access to the EPR or other supporting applications.

3.11.3 Capacity and storage

The system must have adequate data storage capacity to meet likely current and medium term future needs for storing their EPRs and supporting applications securely.

3.11.4 Physical security

The system must be sited in a safe and secure location. Backups must be performed regularly and stored securely (e.g. fire-proof safe designed to protect electronic media). You should take physical security measures to prevent loss or failure of the system due to;

- Theft
- Fire, flood and other disasters whether natural or man made.
- Mechanical, electrical or magnetic damage
- Power failure
- Failure of external systems or dependencies (cables, remote servers).
- Computer viruses
- Staff problems (e.g. illness or absence of system manager)
- Access control
- Damage or destruction of the physical building in which IT systems are held.

Practices must ensure that access to clinical information is controlled so that only those authorised to do so can have access to some or all parts of the clinical system.

3.11.5 Security policy

The practice should develop and implement a security policy in collaboration with their PCO.

3.11.6 Disposal

Practices and PCOs should ensure that they properly manage computers and storage media (e.g. hard discs, cd-roms, tapes, floppies etc) that are no longer required, ensuring that no such hardware contains any personally identifiable patient information before disposal. All storage media should be re-formatted to delete any personal information as per your supplier's instructions before disposal. If there is any possibility that such information might remain accessible on the storage medium after formatting, then you should physically destroy the hardware before disposal.

3.11.7 Disaster recovery

Practices should prepare a detailed disaster recovery plan before they are able to move to paperless practice. To be effective the elements of a disaster recovery plan should include the following:

- Backup of the system to a suitable medium (usually magnetic tape) at regular intervals with a frequency of no less than once per day.

- A system of cycling multiple media such that a single failed backup cannot render the plan ineffective (e.g. using different tapes for each day in a weekly cycle).
- Secure storage of backup media to protect against accidental damage (e.g. flood or fire) or theft.
- A system to ensure that at least one recent backup is retained off-site to provide additional resilience against accidental destruction or theft (e.g. taking the previous day's backup off-site each evening).
- A system to ensure that any warnings or messages produced by the backup system are noted and acted upon.
- Regular replacement of backup media in accordance with the manufacturer's instructions.
- Periodic submission of a specimen backup to an external verification service (where available) to ensure that backups obtained are able to be used to restore a functioning system.

However traumatic it may be, hardware can easily be replaced, but years' worth of patient data cannot, unless it has been properly and verifiably backed up, securely stored and recovery-tested.

3.11.8 Business continuity planning

Many practices are in vulnerable locations and are subject to higher than normal physical risks, such as burglary and arson. Organisations should consider the impact that loss of premises would have on their operations. Modern businesses typically dovetail their arrangements for disaster recovery with a business continuity plan.