Good Practice Guidelines for General Practice Electronic Patient Records

Prepared by

The Joint Computing Group of the General Practitioners' Committee and the Royal College of General Practitioners

Sponsored by

The NHS Executive
General and Personal Medical Services Branch

Date: 31 August 2000

Version: 2.6

1 Foreword

This set of good practice guidelines was prepared at the request of the NHS Executive in consultation with the Joint Computing Group of the General Practitioners' Committee of the British Medical Association and the Royal College of General Practitioners. Its primary purpose is to provide a professional framework for the legitimisation of electronic patient records in general practice. It is also intended as a source of authoritative advice for those general practitioners who keep computerised patient records or who intend to transfer their record systems to computer.

The principles of migration from paper records to electronic records (EPRs) were set out by the joint statement of the RCGP and GPC of the BMA:

- Paperless Practice; a position statement from the Joint Computing Group of the GPC and the RCGP

These good practice guidelines take this statement further drawing on a large body of underlying work which is referenced within “ScopeEPR” below. The principle sources were:

- Computerised Patient Records in General Practice: - Discussion of Good Practice Version 1 David Markwell in conjunction with the Joint Computing Group March 1995
- "ScopeEPR": Royal College of General Practitioners Health Informatics Task Force Electronic Patient Record Study December 1998
- Guidance on Medical Records D E Pickersgill GMSC Statutes and Regulations Subcommittee 1994
- Issues arising from going paperless A Preliminary Report to the Clinical Systems Group Tom Davies – 9th December 1998
- Security in Clinical Information Systems BMA 1996.
- Security Policy for Information and Information Systems in General Practice. Royal College of General Practitioners 1997
- Confidentiality: Providing and Protecting Information. General Medical Council April 1999
- Protecting and Using Patient Information – A Manual for Caldicott Guardians
- The NHS IM&T Security Manual
- General Medical Practice Computer Systems Requirements for Accreditation – RFA99 NHS Information Authority October 1999

The document is divided into:

- An Introduction: which discusses general aspects of electronic patient record keeping.
- The Guidelines: which contains the body of the document.

2 Introduction

The guidelines for good practice described in the next section are based on consideration of the purposes for which patient records are held as identified below:

2.1 The purposes of patient records

2.1.1 Clinical purposes

Practices currently require a patient record system that can be used to:

- Assist in the clinical care of individual patients by:
    - Assisting the author to structure his or her thoughts and make appropriate decisions;
    - Acting as an aide memoire for the author during subsequent consultations;
    - Making information available to others with access to the same record system who are involved in the care of the same patient;
    - Providing information for inclusion in other documents (e.g. laboratory requests, referrals and medical reports);
    - Storing information received from other parties or organisations (e.g. laboratory results and letters from specialists);
    - Transfer the record to any NHS practice with which the patient subsequently registers.
- Assist in the clinical care of the practice population by:
    - Assessing the health needs of the practice population;
    - Identifying target groups and enabling call and recall programmes;
    - Monitoring the progress of health promotion initiatives;
    - Providing patients with an opportunity to contribute to their records;
    - Supporting medical audit.

2.1.2 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 or breach of service);
- 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 PCG;
- Providing evidence of workload to Health Authorities (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).

2.1.3 Additional purposes

Some practices also currently 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 enable:
    - Epidemiological monitoring;
    - Surveillance of possible adverse effects of drugs;
    - Clinical research.

2.2 Electronic and Paper Records

Most of the purposes described above are generic. In other words, they apply to both paper and electronic records. A few, however, are not in that they are only possible in an electronic environment; and some purposes are more easily fulfilled in an electronic record than a paper one and vice versa. What follows is a brief description of characteristics that are, or may be quite different in electronic patient records than in paper ones and which accordingly need to be supported by these good practice guidelines.

2.2.1 General Characteristics

- Physical
  - EPRs depend for their existence on the presence of supporting hardware and software. Paper records do not. In so far as EPRs have a physical presence, this exists at the point(s) of data storage on the machine(s) involved. Paper records exist in the space that they themselves occupy.
- Accessibility
  - EPRs may be available to the clinician at any point where electronic access is provided to the record data (and they allow simultaneous access by several clinicians at different sites). Paper records have to be physically present at the point of use.
- Resource
  - Paper records are cheap in themselves; in comparison EPRs are not. EPRs require investment in the necessary hardware, software, maintenance, upgrades and training. This may be offset against savings in filing, storage and retrieval costs for the paper equivalents but there remains a different order of investment type and magnitude for computerised records.
- Predictability
  - Paper records are highly predictable in their form and function. In U.K. general practice it is perfectly possible for a primary care clinician to move from one practice to another without experiencing any difficulty in reading from or writing to different practice’s written records. This is not necessarily the case for EPRs where not only may the interface to the records be quite different in different practices but, in addition, the added value functions that EPRs may have - such as decision support or audit functions – may or may not be present or be present in unpredictable ways. This has implications for both training and system accreditation.
- Maintenance
  - Paper records require little maintenance beyond consideration of filing and internal ordering. EPRs have all sorts of additional needs in terms of technical maintenance, upgrades, and preservation of their integrity which require quite different organisational approaches and investment.
- Training
  - Paper records are generally regarded as intuitive in their use. Although clinicians typically receive a degree of 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 that additional training investment both because individual EPR systems are idiosyncratic in their construction and require specific training for their use, and because full exploitation of the potential of EPRs requires some understanding of the more general possibilities inherent in computerised records vis-à-vis paper.

2.2.2 Record Characteristics

- Data Entry
  - Data entry in paper records is relatively easy. Data entry for EPRs is more complex, not just because EPR systems require specific training in their use, but also because there are particular problems presented in terms of entering data into EPRs from remote sources, and from the different semantic implications of information in an EPR to that in a paper record. This latter factor is amplified below.
- Data 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 .
- Semantics
  - 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. Their design 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.

2.2.3 Legal Characteristics

While, for the most part, the principles of behaviour that underpin legal aspects of medical record keeping are similar for both paper and EPRs, there are significant differences in the effects of the law on principles of good practice for computerised records vis-à-vis paper ones:

- Medical Confidentiality
  - There is no law in the U.K. that directly asserts the obligations of medical confidentiality. However, any information held in confidence, as is the majority of heath information, is protected by the Data Protection Act 1998 and by the Common Law Duty of Confidence.
- Access to Records
  - Access to both electronic and paper records is now covered by the Data Protection Act 1998.
- Medicolegal
  - There are two aspects of the law as it affects medicolegal characteristics of records that provide for significant differences between paper and computerised records. The first of these relates to the apparent greater ease with which computer records can be modified without that being apparent. To prevent such modification from tainting evidence in court, the Civil Evidence Acts have a provision – see below.
  - The second matter is the question of where lies the true account of events for any case at issue. For a paper record this is usually obvious. It is much less so for EPRs and current law does not help in this regard. This will be discussed further below.

- Health and Safety
  - Paper records have no specific health and safety implications. The machinery which provides access to EPRs is covered by EU directive and U.K. legislation. Once again, this will be amplified below.

2.2.4 Security Characteristics

The differences between paper and electronic records are, perhaps, most marked when security of those records is considered. The subject of record security can be a contentious one; possibly because "security" is not a simple concept in its own right but is made up of different elements. For the sake of definition in this document, the elements of computer security in the Open Systems Interconnection Model of the International Standards Organisation[1] are used. The baseline security standard for the NHS is likely to be BS7799(Part 1: Code of Practice for information security management). Existing guidance can be found in the NHS IM&T Security Manual.

- Availability *(The property of being accessible and useable upon demand by an authorised entity.)*
  - As mentioned above, paper records are available if they are physically present, and EPRs from any point of electronic access. The availability of EPRs is therefore determined by a series of considerations whose total effect on good practice is significant – see below.
- Integrity *(The property that data has not been altered or destroyed in an unauthorised manner.)*
  - This has specific requirements for EPRs which include appropriate audit of record entry/modification as well as physical security of record systems – see below.
- Accountability *(The property that ensures that the actions of an entity can be traced.)*
  - For a paper record this amounts to the "signature". In EPRs, the issues include audit trails and appropriate "authentication" of record entries – discussed at greater length below.
- Confidentiality *(The property that information is not made available or disclosed to unauthorised individuals, entities or processes.)*
  - Finally comes the complex question of maintaining medical confidentiality in and between computer systems, including access control measures, physical security and privacy of systems, encryption and so on. All of these present quite different problems to those relating to confidentiality of paper records.

[1] ISO 7498/2, International Standards Organization, *Information Processing Systems - Open Systems Interconnection Reference Model, ISO 7498/2 Security Architecture*, 1988

3 Good Practice Guidelines

This part of the document contains guidance for general medical practitioners using electronic records as their primary means of keeping information related to the care of their patients. It is this part of the document that is referenced by The National Health Service (General Medical Services) Amendment (No.4) Regulations 2000 which concerns the legitimisation of electronic patient records in general practice. It provides detailed good practice advice in support of aspects of electronic record keeping raised in the Introduction. That advice will, of necessity, change from time-to-time depending on technologies currently pertaining in general practice records, and new legislation that might in future affect the keeping of records in primary care. The guidelines are considered under the following headings:

- Hardware Requirements
- Electronic Record Requirements
- Maintaining Security
- Medical Confidentiality
- Training and Other Resource Requirements
- Regulatory Requirements

3.1 Hardware Requirements

The particular hardware/machinery that is needed for practices to support electronic records will vary to some extent depending on practice circumstances. What follows are some general guidelines that will usually be necessary to consider in each practice's case.

3.1.1 Accessibility

Practices will need to provide for themselves workstations at each point within the organisation where staff will need to have access to the electronic patient record or other supporting applications. This will normally mean supplying workstations in each consulting room, including treatment rooms, as well as in proximity to support staff work locations. The latter would be normally expected to include each fixed place where a receptionist would normally interact with a patient, both physically and on the telephone; each place where secretarial duties are performed; and each place where practice management routinely occurs. Other access points might include a dispensary, portable access for those engaged in household visiting, from the home of some staff, and points of access from allied organisations such as Out-of-Hours centres. (In the latter three cases, it is important to ensure that aspects of good practice are maintained as soundly in those places as they are in the primary organisation with responsibility for the records).

Enhanced authentication mechanisms are likely to feature in future for both NHS staff and patients who access, use and share electronic information based upon "best commercial practice". Such mechanisms will be dependent upon the prior establishment of core infrastructure arrangements for authenticity and trust. They are likely to be similar to arrangements currently being considered for Information Age Government and its interfaces with UK citizens and other organisations.

3.1.2 Capacity and Storage

Each practice should ensure that it has available to itself sufficient data storage capacity (either in terms of hard disk size or other removable or archive media) to meet the current and medium term future needs for holding their electronic records and supporting applications. In addition, they should ensure that the back-up media that they use will meet not only their current requirements but also those envisaged in the medium-term.

Each practice will need to form its own judgement on necessary capacity which will depend on a variety of factors including:

- Practice list-size
- Practice turnover of patients
- The size and complexity of the software that the practice uses
- The data storage efficiency of the primary electronic patient record software

- The degree of detail that the practice typically employs in its electronic records
- Those components of the practice's activity which it wishes to make paperless and the timescale that it wishes to adopt
- The degree to which the practice stores high-volume files in association with their patient records such as image or sound files and, in particular, scanned records or elements of records

That judgement needs to be regularly updated so that, for instance, the practice can be certain that during any 6 - 12 month period they are not going to experience reduced efficiency of the EPR system as free storage space diminishes.

3.1.3 Supporting Hardware

In addition to the central processing unit(s) and access workstations, the practice will need to provide for itself a number of other pieces of equipment. These will include:

- Printers
    - In addition to supplying printers at each place where FP10s will be printed, practices will need to provide additional printing support – usually available across a network to all – for the printing of letters, patient records or parts of patient records, and other documents necessary for the support of the business of the practice.
- Equipment for local network support
    - In order for electronic records to be available from many places in the practice, the practice will need some form of cabled infrastructure. This would normally be expected to be in the form of a local area network (LAN) with appropriate network hubs and cabling. Where practices exist on more than one site, they will also need to support this network across intermediate telecommunications links of one sort or another. Remote accessibility and support functionality are likely to be provided within the new information security architecture in a consistent way and will in future benefit from enhanced authentication arrangements as described above (3.1.3). The NHS Executive will publish further guidance at the earliest opportunity.
- Equipment for remote network support
    - Each practice will need to have the means of access to or from a remote network. This might be the NHSnet, or facilities for remote access for the purposes of maintenance, or the Internet. In each case, at least a modem will be necessary as well as additional equipment for the maintenance of the security of the practice system. The latter is discussed further in the relevant section.
- Equipment necessary for Health and Safety
    - Each Visual Display Unit (VDU) that the practice uses will need to comply with the relevant law (see Regulatory Requirements). In addition, the practice would be well-advised to ensure that the ergonomic characteristics of their work-terminals are appropriately maintained. This may mean providing special office furniture including adjustable seating, adjustable arms for display equipment, purpose-designed desks, VDU screens and so on.
- Equipment necessary for Security
    - In order to maintain the physical security of the system, the practice will need additional pieces of equipment. These would be expected to include:
        - Uninterruptible Power Supplies (UPS) (which need to be used not just for the main processing unit but also for any terminal where significant additional processing occurs)
        - A fire-safe for the local holding of back-up and other sensitive removable media
        - Additional security material such as desk chains, lockable boxes for main processing unit(s), movement alarms and so on

3.2 Electronic Record Requirements

This part of the good practice guidelines expresses advice on a number of aspects of good record-keeping that are peculiar to electronic systems. It does not constitute a general treatise on good medical records. Each aspect is discussed under its own heading:

3.2.1 Expression of Information

All medical records are more or less successful depending upon their ability to communicate to others, to their authors over time and, now, to their subjects what was the essence of the patient's condition and experience and the clinician's appreciation of them at the time of recording. EPRs, in addition, may be deemed to be successful if they appropriately provide the wherewithal for secondary processing of the information within them either for the purposes of medical audit, decision support or secondary display of categories of clinical information for particular purposes. This inherent aspect of electronic patient records can only occur if the records are provided with a machine-recognisable "structure" in the form of medical codes, clinical headings or categories, standard qualifiers of information and so on. The need for this "structure" in an EPR, while facilitating its inherent added value, also means that the entry of data may need to be facilitated by the use of constraints (and hence the expression of information) needs to be constrained.

Furthermore, information entered into one patient record system will ultimately be transferred in whole or in part to another where it is important that the meaning of the original entry be preserved. This fact carries further constraint.

Some issues arise:

1. **Code use policy**: It is already a matter of professional and public policy that general practice (and all N.H.S. EPR systems) should use a common coding scheme so that machines may share an understanding of the medical concepts that the coding scheme represents. This policy has not yet been achieved but it has recently been re-avowed in the NHS Executive Information Strategy *Information for Health*. One mechanism for introduction and maintenance of a common coding scheme in general practice could be through the Requirements for Accreditation for G.P. systems (see below). This already requires G.P. systems to use one of the versions of Read codes.

   However, even when a common coding scheme is in place (as it usually effectively is on any single EPR system), there will be a number of possible ways to express what amount to similar concepts. This may have little significance as far as the subsequent human-readability of the information is concerned but, if a practice wishes to perform retrospective audit or other machine processing based on the value of the codes used, difficulties may arise in construction of reliable queries. Hence it would be advisable for practices who intend to perform such audit regularly to agree in advance what will be the permissible code values to be used at the point of data entry (and possibly to constrain that data entry by the use of some template or device which enforces a particular set of code values).

   In addition, in most current G.P. systems, there is usually a wide degree of choice as to how much of the information to be entered can be done by means of "free text" and how much can be entered using coded entries or a combination of the two. Views on the correct balance between these two models is evolving.. The more coded data that is entered, the easier the record is to manipulate, with more meaningful interrogation being possible. In addition the more coded the EPR becomes the greater the potential value of any subsequent onward transfer. On the other hand clinicians need to have the freedom of expression that comes with unlimited free text entry.

   Many entries are records as to fact; for example what the blood pressure was on a particular day, or a full blood count result or some other measurement, or the confirmation of a myocardial infarction. In any particular practice, it would be advisable that a consensus is reached as to which categories of entries should always be coded. Other types of entry may not need to be so stringently coded but all entries may have their value enriched with added text.

   The diversity of practice is such that there will probably always be information for which a definitive code cannot be found. Subject to 3 and 4 below, more general codes might be used with free text amplification or for some entries non specific general codes (such as the code "had a chat to patient") might be chosen to which the clinician may or may not wish to make an appropriate text entry

   Where codification of certain data is not felt to be sufficiently important a practice may decide to use only free text entries. .

2. **Maintaining coherence over time**: Just as in paper records it is deemed good practice to maintain an up-to-date view of the record as a "summary" or "problem page" which is itself internally coherent and accurate, so are there equivalent aspects in electronic patient records. They include:

   - Maintenance of accurate episode/problem titles: Where a developing clinical situation means that, for instance, a problem that presents as "polydipsia" is subsequently confirmed to be due to "Diabetes Mellitus", that change should be reflected in the title of the problem and all subsequent entries that are made relating to it. This should preferably be done by changing linkage priority within a record rather than changing original record entries (and hence altering the original apparent perceptions of the author).
   - Maintaining appropriate currency of problems: Similarly, where a system has the ability to denote problems as having currency or otherwise (i.e as being current or active), regular review and changing of inappropriate status should be performed.
   - Maintaining appropriate links between episodes and problems: where record entries are made over time for what amounts to a similar problem, that linkage should be maintained.
   - Maintaining appropriate links between problem/diagnostic codes and related therapeutic events: where it is possible to link medication or other interventions to the relevant diagnosis or problem code, that link should be included at the time of data entry.

3. **Major modification/qualification**: When coded information is entered into an EPR, it is possible to alter the apparent meaning of that code either by entering qualifying text against its rubric, or by adding some qualifying code which specifically exists either on that system or within the coding scheme used. In the latter case, provided that the system appropriately represents the changed meaning both in human display and in any subsequent query, no danger arises. However, if one considers examples such as "F25.. Epilepsy" qualified by the text: "excluded by AV/EEG monitoring", or "7AH.. Hysterectomy" qualified by the text: "not performed", it is not difficult to see the problems that might arise for the patients in whose records such entries exist. If those records are then passed to a different system which recognises the codes but not the qualifying text, then the potential danger becomes magnified. In short, while it is entirely acceptable to use free text to amplify the concept represented by a code, **it is never acceptable to use free text to modify the fundamental meaning of a coded entry.**

4. **Free text and auditability**: Another danger of free text entry is the potential "loss" of information that might otherwise have been separately codified. If a coded entry for a Faint is chosen and the patients blood pressure is typed in as free text this may present a visually acceptable record but that blood pressure will not be recalled by any subsequent search of that patients EPR that looks (logically) for all coded blood pressure entries. Thus not only should free text not materially modify the meaning of the coded entry neither should data that has its own significance be recorded as free text.

5. **Validity of record entries**: The issue of retention of records is dealt with elsewhere. Practices need to ensure EPRs are correctly constructed and this is a dynamic process. There may be occasions where entries might be considered for deletion, but this is generally unacceptable unless required by Court Order or legislation (e.g the Data Protection Act 1998). If an entry is or becomes invalid ideal practice would be to make that fact apparent by invalidating but not removing the entry - with appropriate comment as necessary. It is not possible to do this on most current systems within the visible EPR, although it is a requirement that all record modifications should be recorded in an audit trail. For the moment, this means that any records that are archived within the practice must include their own audit trail within the archive. Future system design will need to allow visible invalidation of record entries also.

3.2.2 Entry of data from sources remote from the practice

If a practice decides that it will use its computerised records as the primary source for all information on a patient, then it will need to address how it will capture record information arising from outside the practice. Broadly speaking this information fits into three categories:

- Information coming from consultations outside practice premises (e.g. home visits, OOH contacts)

- Information coming from secondary care or other parts of the broader health service
- Information coming from a previous practice.

In most of these cases, the electronic transfer of that information has the potential to obviate this difficulty. However, such facilities do not yet exist except for a relatively small number of information flows. Consequently, the practice will need to develop a policy as to how this information will be captured and identify resource to enable it.

In the case of primary care consultations happening outside the practice, the essential details of those should be transcribed into the EPR as soon as is reasonably possible thereafter so that no crucial element of the patient's recent medical history is missing at a subsequent consultation.

Discharge and out-patient letters, investigation results and the like should also have their details entered into the EPR. In the case of investigation results, these should be entered directly into the EPR in a form as close to the original as possible. Information from letters may be summarised in its essentials according to protocol and transcribed, it may be scanned as an image file, or it may be optically character read to produce an equivalent text representation. In the latter case, practices should be aware that OCR technology is fallible and that consequent errors – particularly in numeric information - may have adverse consequences. Where text based communications are scanned or manually entered into the EPR any substantive investigations or results that are reported or referenced within the text of the communication should be entered under a separate and appropriate coded entry. For instance a discharge summary for a day case angiogram might be entered as a scanned document but in addition an entry should be made in the EPR using the appropriate angiography code.

Previous G.P. records are usually too bulky to efficiently transcribe in their entirety and, accordingly, they will need to be summarised and, where appropriate, coded by a competent person or persons under instruction by protocol. It would also be wise to enter the fact of their having been summarised into the record (and to keep the full record available for more detail when appropriate).

Whether a practice should destroy documents that have been transcribed into a computer system remains unanswered. The decision rests with the individual practice but they should bear in mind that medical defence organisations advise that original material should not be removed from records.

3.2.3 System accreditation

No mention is made in these good practice guidelines of specific software requirements for EPRs (beyond those described generically such as word-processors, virus checkers etc.). The reason for this is that, where there are particular technical requirements necessary for the support of general practice, these would be expected to be defined in the current version of the Requirements for Accreditation for G.P. systems. This mechanism does not purport to be a tool for expressing preferences for usability but it should include specifications of matters relating to the safe and reliable processes necessary for patient care on general practice electronic systems.

The regulatory framework which underpins the change from paper to electronic records specifies that GPs must use clinical systems which are accredited as meeting the Requirements for Accreditation (RFA99) standards as a precondition of moving away from paper records.

3.3 Maintaining Security

3.3.1 Security Policy

The practice should draw up and follow a security policy that takes full account of the need for confidentiality (see next section), authentication and integrity of the computerised patient record system. The practice security policy should take account of local circumstances and risks but should specifically address the points under the headings below.

The practice will already have a Caldicott Guardian as part of its parent PCG/PCT, but that person's role is confined to a local determination of good practice as far as access to patient-identifiable information is concerned. The issues relating to security of computerised records go further than that and it is important that this should be recognised as part of the policy.

The newly formed National Body on Confidentiality will play a significant role in advising and setting of standards in the future.

3.3.2 Authentication and Accountability

The practice security policy should recognise the need for data entry to be restricted to properly trained and authorised people. It must take full account of the need for entries to be accurate, complete and attributed to the person responsible for the observations or interventions recorded.

When considering the issue of authentication, health professionals should be aware that they may be held liable for the content and accuracy of information that appears to have been entered by them or on their behalf. It is therefore important that the security features of the system and procedures followed by the practice combine to minimise the risk of a record entry being accidentally or fraudulently attributed to the wrong user. Practices should be aware that it may be necessary to prove that an entry was or was not made by the person to whom it is attributed. This means that, since most record entries are logged as being the responsibility of the individual whose password is currently entered, it should never be acceptable for an entry to be made into a record when someone else has logged into the system. More generally, it is essential that all users:

- Have a unique user identity and password;
- Keep their password secret and do not divulge it to other users for any reason;
- Change their passwords at frequent intervals;
- Log out of workstations when their task at that workstation is finished and never leave a workstation logged in but unattended.

The practice policy on data entry may allow another person to make entries in the patient records on behalf of the responsible healthcare professional. The information on which such entries are based may be a written note, a dictated message or a verbal report by the healthcare professional responsible for the observations or interventions recorded. Entries made in this way must be:

- Transcribed to the computerised record by an authorised trained person who ascribes the entries to the healthcare professional who wrote or dictated the notes;
- Monitored in accordance with the practice policy on data entry to ensure the accuracy and correct attribution of the entries made.

The practice system should record details of who, what and when was recorded in an audit trail according to the current version of the Requirements for Accreditation (see Regulatory Requirements).

If reports and correspondence are received electronically from outside the practice, the practice policy should include procedures to ensure that:

- All information received is seen by the person responsible for the original request or by another doctor acting on his or her behalf;
- The information received is filed in the computerised record of the patient to whom it relates.

It is also likely that authentication measures for electronic medical records and their products will be supported by electronic signatures in the medium term future. These guidelines would then need to be updated.

3.3.3 Integrity and Availability

The practice should protect the patient record system from physical and operational threats to its integrity. Some of the equipment necessary to protect the record system is mentioned above under Hardware Requirements. More generally, physical security measures should be applied to prevent loss or failure of the systems due to:

- Theft;
- Fire, flood and other natural disasters;
- Mechanical, electrical or magnetic damage;
- Exposure to environmental factors outside the limits recommended by the manufacturer (e.g. excessive heat, cold, humidity or dust);
- Deliberate tampering with or deletion of files:
  - Audit trails should be capable of detecting tampering and should be secured against deletion.
- Computer viruses:
  - Disks received from outside the practice should be checked for viruses by effective and regularly updated anti-virus programmes;
  - Files received from outside the practice by electronic transfer should also be checked for viruses.

Measures designed to protect the integrity of the system must take account of the risks of:

- Malicious damage by disaffected staff;
- Non-availability of necessary information due to:
  - Loss of keys or passwords by users;
  - Illness, death or disaffection of the only person who knows the password that grants access to system maintenance facilities.

In addition, the practice should have an insurance policy sufficient to cover total system loss and its consequent effects upon the practice organisation.

The normal operation of the computer hardware and software should be protected by maintenance agreements that guarantee a rapid response to faults caused by component failures and faulty software. The service levels specified in the Requirements for Accreditation of General Practice Computer Systems (RFA99) are a minimum applicable to practice management systems. Higher levels of service are desirable for a computerised patient record system. It is also highly desirable that one or more staff within the practice have sufficient I.T. competence both to deal with relatively minor operating problems when they arise, and effectively to liaise with support staff if more major difficulties are present.

The practice should have a clearly laid out disaster recovery plan. This will need to address the temporary replacement of the practice's electronic functions with paper based alternatives, the retention and subsequent entry of these temporary records into the electronic record system when it becomes available again and the extraction of essential information from ancillary systems such as any electronic appointment book's backup.

Procedures to make backup up copies of the patient record system must be:

- Appropriately planned to ensure that a valid recent copy can be recovered;
- Regularly, correctly and consistently carried out;
- Verified by checking the integrity of the backed up data (on every occasion).

Used backup disks and tapes should be replaced with new media at regular intervals taking account of the manufacturers recommendations on the anticipated working life of the media used. Old backup media should be re-formatted or physically disrupted so as to render any data on them unrecoverable.

If the backup procedure offers a choice of backing up different parts of the system, the routine backup procedure should always include a backup of the audit trail.

Media containing backup copies of the patient records should be kept secure against theft and damage. To ensure the safety of backup copies, the most recently recorded backup media, should be stored in a fireproof safe in the practice premises. At least once a week, a full backup copy should be taken to and stored in a secure location. This location should be neither in nor immediately adjacent to the practice premises (e.g. a fireproof safe at the home of one of the partners). At any time there should be at least:

- Two complete backups (both less than four days old) stored in the practice premises;

and

- Two complete backups (both less than fifteen days old) stored at the other secure location.

Fireproof safes used for this purpose must be certified as appropriate for magnetic media. A fireproof safe that is adequate for the storage of paper may not protect its contents from temperatures that will destroy backup disks and tapes.

3.3.4 Retention of Records

Whenever and wherever an entry is made into a computerised patient record, the information entered must be retained by that practice in the form in which it was entered for an appropriate period of time. This information must be retained even if a copy of the computerised patient record is transferred to another practice. There are, as yet, no absolute rules as to what is "an appropriate period of time". The period for which records may be retained depends on the purposes for which they are to be used. Current recommendations from the Department of Health[2] are that medical records should be retained for the following periods:

[2] (HSC 1998/217: Preservation, Retention, and Destruction of GP General Medical Services records relating to patients)

- **Maternity records;**

  25 years.

- **Records relating to children and young people (including paediatric, vaccination and community child health service records);**

  Until the patient's 25th birthday or 26th if an entry was made when the young person was 17; or 10 years after death of a patient if sooner.

- **Records relating to persons receiving treatment for a mental disorder within the meaning of the Mental Health Act 1983;**

  20 years after no further treatment considered necessary; or 10 years after patient's death if sooner.

- **Records relating to those serving in HM Armed Forces;**

  Not to be destroyed.

- **Records relating to those serving a prison sentence;**

  Not to be destroyed.

- **All other personal health records;**

  10 years after conclusion of treatment, the patient's death or after the patient has permanently left the country.

The Data Protection Act can be interpreted to suggest that computerised records should not be kept once the individual concerned is no longer receiving services from the organisation concerned. This is clearly unacceptable from a medicolegal standpoint both as far as patient and clinician are concerned. The Data Protection Commissioner has accepted the BMA's advice that until such time as a patients electronic record (with its associated audit trail) can be reliably transferred between practices a practical interim solution is required. If the patient is no longer receiving services from the practice their record should be made "inactive" or archived. Inactive records should not be accessible in routine use of the system. They should only be accessed in response to a new request for service or some other valid reason. Whenever an inactive record is accessed a record of why that access was made must be kept. It follows that in the meantime practices should never delete any EPR they have created or been responsible for.

3.3.5 Transferring records.

Ultimately an EPR from one practice should be transferable to another with no loss or corruption of its content and functionality. Work on such systems has begun with the Department and initial text based transfers should be possible by early summer of 2001. This will be followed by further work over a period of about two years to develop a system which will transfer the EPR with full functionality being retained. If in the interim a computer supplier delivers this functionality for use where the sending and receiving practices have a common computer system, its use by practices with electronic records will be subject to the agreement of both the sending and receiving practice and adequate security procedures. When transferring a patient's record, the origin of the transfer must be authenticated in the transfer message and the transfer must be logged in the audit trail of the sending and receiving systems.

When transferring a patient's record, each entry within the transfer must contain sufficient information to identify the practice from which it originated. If it is necessary to verify the authenticity of an individual entry or group of entries, this can then be done by reference back to that practice.

When entries are received from another practice, these should be added to the patient record but should not overwrite any existing entries. This is particularly important if some of the entries were originally made in the receiving practice and have been copied to the sender in an earlier transfer.

When a patient registers with a GP in another practice the information in his or her "current" computerised patient record must be sent to the practice at which the patient is now registered. When appropriate facilities are available for electronic record transfer, the information should be sent in that form. Otherwise a printed copy of all the electronic record must be sent.

If a GP leaves a practice partnership while retaining his list of patients, the information in the "current" computerised patient records of all patients on his or her list must be made available to the GP who is leaving the practice. If appropriate facilities are available the information must be provided in an electronic form. Otherwise a printed copy of the record must be provided.

A GP from a practice with whom the patient is not registered may be consulted by a patient for several types of service. In these cases the GP should make an "interim" computerised patient record in which to make entries related to the services provided. For the purposes of determining the way in which entries made during these consultations should be handled the services are divided into two categories:

- *Short-term services* include:
  - Temporary registration;
  - Immediate necessary treatment;
  - Emergency treatment;
  - Out of hours cover.
- *Stand-alone* services include:
  - Maternity registration;
  - Contraceptive services;
  - Child Health Surveillance.

When a *short-term service* is completed, a copy of the information in the "interim" record must be sent to the authorised holder of that patient's "current" record.

When a *stand-alone service* is provided, a copy of the information in the "interim" record must only be sent to the authorised holder of that patient's "current" record with the patient's explicit consent.

3.4 Medical Confidentiality

The practice security policy must recognise the rights of patients to insist on the privacy of their medical records and should take account of:

- The provisions of the Data Protection Act 1998 relating to the confidentiality of personal information stored in computerised systems and in particular the requirements for processing to be both fair and lawful;
- The Common Law Duty of Confidence, including the need for informed consent;
- Ethical guidelines specific to health information.

The practice should prevent accidental or deliberate access to the records it holds by unauthorised people or organisations. The practice should use physical security measures to prevent unauthorised access to:

- The surgery;
- Computer(s), workstations and communication equipment;
- Backup media containing copies of patient records.

The practice should make use of technical restrictions on access to the patient record system provided by their system. Technical restrictions on access to the patient record system should include:

- Passwords or other proofs of identification such as smart cards and PIN codes;
- Different levels of access according to the professional status of the user;
- Automatic disconnection after a period of inactivity.

If these features can be configured, this must only be undertaken by a person authorised by the practice. The configuration must be set in accord with the practice security policy.

Additional restrictions should be applied to remote access to the computerised patient record system. The measures that should be applied include:

- Regular disconnection of the modem (or use of facilities for disabling modem auto-answer) when remote access is not required;
- Ensuring that the numbers associated with any dialup access lines are ex-directory, known only by those who are authorised to access the system and cannot be easily deduced from published practice phone numbers (i.e. not an adjacent number);
- An automatic log recording attempts to access the system from outside the practice. This log must be regularly reviewed to detect unusual patterns of access.

Other measures that should be considered include:

- Use of dial back modems;
- Use of modems that encrypt all interchanges;
- Installation of a firewall between the clinical system and any outside network which may be accessed from a common terminal (this is to be undertaken as part of the connection of GPs to NHSNet).

The practice should apply organisational and procedural measures to prevent unauthorised disclosure of information. These measures should include:

- Confirm the identity of the requester;
- Verify that the address to which the information is to be sent is appropriate to that requester;
- Ensure that the requester has a valid need for or right to the requested information;
- Ensure that transferring the requested information does not breach the Data Protection Act or ethical guidelines relating to the patients rights to privacy, e.g obtaining consent where necessary;
- Ensure that restrictions imposed by patients on the disclosure of confidential information are effectively recorded and respected unless there are overriding legal or ethical considerations;
- Use an appropriate secure method to transfer the information while minimising the risk that any sensitive information will reach or be intercepted by a party other than the intended recipient;
- Maintain a log of all transfers of information, including a record of the information transferred and the identities of the requester, the destination and the person authorising the transfer;
- Training all staff with access to the record system to ensure that they are aware of their responsibilities for confidentiality of patient records;
- Appropriate provisions in staff contracts specifying disciplinary rules in respect of breaches of the Data Protection Act and/or other specified guidelines on patient confidentiality;
- Positioning of screens and printers to ensure that printed or displayed information is not visible to unauthorised people during normal operation of the system;
- Clearing a displayed patient record from the screen before a new patient enters the consulting room;
- Secure filing of printouts from the computer system while they are in use and destruction of printouts when they are no longer required;
- Ensuring where practical that all patient-identifiable information (whether by e-mail or as an electronic message) sent across a wide area network is encrypted.

3.5 Training and Other Resource Requirements

Training for health professionals and practice staff is essential to ensure that they will all have the requisite generic and system-specific skills to use primary care EPR systems safely and effectively. This training needs to start before practices go paperless, so that they can fully understand and implement the changes in their own practices in a strategic way. Poor quality data accumulated early in the transition to an EPR will create a legacy not only for the originating practice but also for every practice that subsequently handles that record.

There should be a consensus that underpins an agreed strategy for the practice. Moving from paper-based records to an EPR is not an all or nothing phenomenon. Practices will inevitably migrate from low levels of “Paperlessness” to higher levels. The practices strategy will need to take account of the timescale of their chosen migration. For the foreseeable future, practices will still have to process paper, extracting meaning from various letters, forms and reports whilst building their EPRs. Practices will have to develop the skills to add, edit and process computerised information for individual patients and practice populations linked to individual care, population surveillance, audit, teaching and clinical governance tasks. Clinical computer systems rely upon high quality data entry and traditional practice staff skills will not be sufficient.

When clinical records are computerised there is an inevitable progression for allied systems to be computerised (referral letters, appointments, scanning, internal and external e-mail, accounts, etc.) These systems also have their own training requirements.

What should the practice consider before switching to full EPRs?

- Talk to other practices that are already using electronic records. Learn from their experience. Your PCG/T, HA, system supplier or local user group may be able to help with advice, training and support.
- Using the Local Implementation Strategy processes may help to ensure that appropriate resource support is made available at the appropriate stages in the practices migration to electronic records.
- Make sure your clinical system is up to the job. Is it accredited to the current version of RFA?

- Where are you now? Poor quality paper records might need to be brought up to a level that then enables them to be transferred to electronic form see 3.2.2 .
- Develop a practice training and implementation plan for moving to EPRs. Involve all the staff and health professionals who will have access to the system (including attached staff, locums and any others). Consider the skills mix your practice will need to maintain EPR systems.
- Agree with your Health Authority a staged migration to becoming "Paperless". Different components of the practice's activity that could be recognised as being part of such a migration pathway might be:
    - Use of Registration links
    - Use of IOS links
    - Use of Pathology links
    - All electronic repeat prescribing
    - All electronic acute prescribing
    - Appointments systems
    - Cytology records
    - Immunisation records
    - Basic biometrics recorded in the EPR
    - All investigations recorded in the EPR
    - Previous paper records summarised on the EPR
    - Disease specific or CDM data recorded in the EPR
    - Some or part consultations on the EPR
    - All consultations on the EPR
    - External consultations recorded in the EPR
    - External text based communications entered into the EPR
    - The use of associated electronic information sources and decision support software
- During this transition the practice must understand the importance of the clinicians having access to the entirety of the patients record, paper and electronic. Clinicians may need to have both paper and electronic records available during consultations for as much as two years.
- How do you transfer information from the paper records, letters, reports etc to the EPR? How can you best do this on an ongoing basis for all the paper you will still have to process? Will this be done by staff or doctors? How do you ensure you capture all the relevant information? What technologies will we use to assist us? (e.g. scanner, OCR software, voice recognition software).
- Above all develop EPRs that help you with the tasks of general practice.

At some point in the migration process the revised regulations will require a general practice to formally obtain their health authority's approval to move away from paper based medical records. The GP "terms of service" have never been specific as to what constitutes an adequate record of the illnesses and treatment of a patient. Without such clarity it is difficult to be precise about the point in a migration pathway where formal approval to maintain electronic records would be required. Pragmatically the use of GP/HA LINKS messages has never been seen as being contrary to the old "terms of service" provision and there is no reason for this to change. Equally items such as electronic appointment registers or repeat prescribing should not require formal approval. However, once a practice plans to retain significant clinical information only in an electronic form GPs should discuss the formal approval mechanisms with their health authority.

3.6 Regulatory requirements

These good practice guidelines are an attempt to distil elements of existing ethical principle, the day-to-day experience of modern general practice, and relevant legislation. That legislation covers subject areas which include:

3.6.1 The Misuse of Computers and Computer Data

- Data Protection Act 1998
- The Computer Misuse Act 1990

3.6.2 Patients Rights of Access

- Access to Medical Reports Act 1988
- Data Protection Act 1998

3.6.3 Medicolegal Requirements for Computer Records

- Civil Evidence Act 1995

3.6.4 Health and Safety at Work

- The Health and Safety (Display Screen Equipment) Regulations 1992
- Health and Safety at Work Act 1992

3.6.5 Intellectual Property Rights

- Copyright, Designs and Patents Act 1988

This legislation forms a regulatory framework within which these good practice guidelines sit.

Finally, there are additional sources of guidance in the works referenced in the foreword to this document.