EURIM
Medical Records Group
Status Report
January 2003

Right Data, Right Place, Right Time – Joined-up Medical Records?

Introduction

Quality of healthcare has unique political resonance; health professionals represent the largest human capital investment and health records are the largest mass of personal information stored in the UK. The NHS is the second largest employer in the world with strong traditions of professional independence producing great variety in clinical and management processes. Any major programme to modernise the application of IT in the NHS is therefore likely to be "high-profile", especially since delivery of improved service at affordable cost may well be the most significant test that voters will apply to Government performance at the next election.

Central to any such programme is the provision of accurate patient information, when and where it is needed with a focus on the benefits to the patient - firstly because this is the acid test of any proposed improvement and secondly because of the importance now given to informed patient consent and co-operation.

Progress on the ground - right now

Modern medical care is increasingly dependent on the rapid availability to health care professionals of accurate information on the treatments that a patient is (or has been) receiving from a variety of sources. Such availability generally calls for collation of information from a wide variety of legacy systems, each containing partial information about the same patient using different (often incompatible) coding conventions and structures. Data frequently has different levels of accuracy and confidentiality, and is stored on different computer systems or technologies.

The Government wants patients to be confident that NHS professionals caring for them have rapid and reliable access, 24 hours/day, to relevant personal information necessary to support their care. One way of helping health care professionals is to deliver Electronic Patient Records (EPR) at the bedside. This allows health care professionals access to up-to-the-minute patient data, including medical records. Armed with all relevant data about the patient, doctors and nurses can make informed decisions and ensure that the patient receives the right treatment at the right time.

Examples of real progress already exist: Chelsea & Westminster uses portable, wireless systems to provide information direct to clinicians at the 'point-of-care' (in most cases, at the bedside). The clinician can interrogate and update patient records while privacy is ensured through fast, encrypted, secure communications. Daily use of the technology stimulates the required culture change, though some people take longer to become comfortable with the system than others.

Benefits and Risks of Data Sharing

Knowledge does not come cheaply, but if good information is expensive, how much greater is the cost of ignorance? Studies and inquiries over the past twenty years indicate that most avoidable tragedies occur because information is simply not available. Less often they occur because information is incorrect or misinterpreted - including by staff transferred from another hospital using a different coding convention. Common complaints by patients include the need to give the same information at each stage of their treatment, or learning by chance or by mishap that essential information has not been passed on. Even if a patient is admitted to a hospital that has treated them before, it is all too rare for the A & E department to have early access to their records, while GPs often lack rapid access to hospital information on their patients and vice versa. Meanwhile, a vast amount of information routinely logged over nearly twenty years by general practice and hospital systems is still not available for use in epidemiological research. The cost of delay and incompatibility, let alone inaccuracy, can be counted in unnecessary suffering and death, not just wasted time or money. We must act now to prevent further suffering and save lives.

Much has been said about the need to protect patient data from abuse, but there is little supporting data on patient views. Last year the NHSIA-commissioned MORI poll results showed widespread support for the open sharing of information between health care professionals concerned with their treatment, (98% happy for their GP to see their record and over 80% for Hospital Medical Staff). However, there was significantly less support for information being made available for medical research, while 43% *opposed* their medical information being available to administrative staff and 36% were against access by social workers.

Public trust in the integrity of the operational practices involved is essential. The role of the support staff who commonly update or access records on behalf of clinical staff and, in consequence, commonly have unchecked access to almost all records, requires formalisation in codes of practice and conduct.

Problems of Data Accuracy and Compatibility

Even where the IT systems handling medical data are of high quality, the classic "garbage in - garbage out" problem applies. Error rates of 10% - 30% have been found in most recent exercises to check the accuracy of data entered by clerical staff into public sector systems (from health care to police and criminal records) where accuracy is supposedly important. Only data entered at the time and place of transaction, by those with a direct interest in its accuracy, is likely to be reliable.

One of the biggest problems in the health service is to move towards direct data entry by health care professionals without increasing their net workload. Another, equally important, is to move towards standard and compatible terminologies from a situation where, not merely may different terms be used, but the same term may mean different things to different people in different systems or situations. Finally, the coding structures used in secondary care are often different between hospital practices - this can be a particular (and occasionally catastrophic) problem for those who may be called on to work long hours shortly after changing hospital or department (such as junior doctors).

There are valid reasons for differences between terminologies and coding frameworks used by different professionals to describe the condition of the same patient. However, it can be dangerous, as well as misleading, if the systems or staff use terms or codes which can have different meanings according to the context in which they are used. The recent NHSIA consultation exercise is therefore most welcome and further work is needed to support the IA initiative.

Similarly, recently established trials of SNOMED (Systematized Nomenclature of Medicine) propose an official standard clinical coding classification and terminology. A final decision on whether SNOMED will become the mandated standard clinical terminology for the NHS is promised once the NHSIA has completed its evaluation early in 2003. This will represent a great step forward at a conceptual level, although the universal adoption and deployment of the coding system will demand much hard work.

Issues of Consent and Data Protection

There is common confusion as to what is required under current Data Protection Act legislation with regard to patient consent to data transfer. The Act does not of itself require the consent of patients to the processing of data for medical purposes. However, because there is a general requirement that all processing of personal data be lawful, and because in many cases the general law (including medical confidentiality) requires that patient consent is obtained for the processing of personal data, then consent becomes an implied requirement of the Act. There is a requirement to inform patients of the identity of the "data controller" for their records, the purpose or purposes for which the data intended to be processed and any further information felt necessary, having regard to the specific circumstances in which the data to be processed, to enable processing in respect of the patient to be fair.

Any data-matching exercise (e.g. to collate patient information from a variety of sources to provide a common, up-to-date record) would need to be lawful. This would require not only compliance with the Common Law duty of confidence but also compliance with other Statute Law determining the functions and powers of organisations intended to be part of the data-matching exercise. The patient must also be given information as to whether the proposed uses or disclosures of data would be mandatory or optional. Failure to provide this information would be likely to result in personal data being unfairly collected.

Many of the systems commonly used by GPs and specialist clinics have long had facilities for "sealed envelope" information available to named practitioners only for when patients may not wish some parts of their medical records to be available to other members of the practice (e.g. young girl on the pill, who does not want any risk of her parents being informed, or an individual with a sexually transmitted disease who may be sensitive about any other than their contact in a specialist clinic being aware). A related issue in this area concerns the use of medical data by the insurance industry, where it may be feared that cover will be refused to patients on the grounds of what they reveal, or indeed refuse to reveal, to insurers. There is a converse problem where the insurer pays for tests, the results of which may not then be available to the patient.

In deciding whether to offer an opt-out, data controllers need to distinguish between those uses and disclosures of data which are essential in order to treat patients within the health service and those which are not. The term “essential” covers those uses and disclosures without which treatment could not be given and those uses or disclosures which the law makes mandatory. In effect, such uses and disclosures are necessary elements of the medical purposes for which that patients’ data is processed. Current guidance from the Information Commissioner is that it is unlikely to make good administrative sense to offer patients the opportunity to object to the processing of their data for any “essential” elements and that it would not therefore make sense to provide an opt-out (including with regard to the ‘sealed envelope’ routines long included in GP health care systems).

Recent hearings in Brussels regarding the possible review of the EU Data Protection Directive indicate that few individuals are aware of their supposed rights and few data controllers understand their responsibilities. Not surprisingly, many now regard the legislation as a bureaucratic barrier to efficient customer/patient service rather than a necessary or desirable protection for personal privacy!

There are a variety of ways in which patients might supply consent to the use of their medical data, including through the use of privacy enhancing technologies (for example, a patient ‘smart card’ could be used to store pre-consent conditions). Before looking at the technologies there is, however, a need to address the means of collecting informed consent, ideally at a time when the patient is not under stress (e.g. during a “routine” visit to their GP) and of checking or updating that consent (e.g. as part of the hospital admissions procedure or during a consultation). Thus a patient who does not want their information to be used for medical research purposes (or for statistical purpose only) might change their mind when offered the opportunity to be part of a trial of a new treatment that could, if successful, improve their quality of life.

Making appropriate data available, while maintaining security

The split of roles and responsibilities between information officers tasked to make information available and data protection officers tasked to prevent abuse (with the consequent risk of adversarial approaches) is considered to be counter-productive. The priority in health care should be the accessibility of shared medical data, when needed, to the clinician. In order to ensure that information remains controlled, the current adversarial structure in which Caldicott Guardians’ work to a set of principles focused on protection should be changed so that an Information Officer would have a Caldicott Guardian to advise on the handling of clinical data (including ensuring that it is available when needed, as well as protected from abuse), with the accountability for the balance between availability and protection subject to external review.

There is also a risk of information overload in circumstances where an individual’s medical history is complex and it will be necessary for certain critical information to be brought to the forefront in presentation of the data so that the key facts of medical relevance are not hidden in a morass of less important data.

Traditional processes for handling paper-based medical records are widely regarded as extremely lax in security terms. From the viewpoint of any individual, there may be a trade off between the current lax state of paper records and the potential for strong electronic security to the electronic data. The status quo offers a curious form of security by virtue of the difficulty that paper records pose for anyone wishing to collate all of “your” data. By contrast, electronic records are more readily collated but can also be more strongly protected! In order to address these concerns, any widespread sharing of data would need to be attended by clarity of policy in three broad areas to ensure that the potential risks are mitigated:

- The legal frameworks whereby potential risks can be covered by existing law or extensions thereof.
- Principles for handling sensitive medical records, which may need to be promulgated, possibly with legal force, to ensure that individuals adhere to good practice.
- Codes of good conduct and practice which are promoted, promulgated, observed and also enforced by those individuals and professional groups who have regular need to share data.

The art of the possible

One of the main challenges is to provide trusted policy frameworks that reconcile the need to share information with pressures to protect that information from abuse. Another is the identification and adoption of realistic strategies for transitioning from the current fragmentation (including of responsibility for action) to the common use of systems which enable the effective sharing of accurate and meaningful information in forms that will be correctly interpreted and used by the recipient.

Success will entail the informed support and consent of healthcare professionals and patients, as well as of would-be suppliers of technology, systems and services, in setting realistic and trusted frameworks within which practical progress can be made. Once consent has been gained, step-by-step progress must be ensured within those frameworks, avoiding the tendency to pursue grandiose “national” projects of the type which have failed so expensively in the past. Nor should we concentrate scarce resources on prestige centres of excellence without considering whether their systems can be replicated or joined up. Politically, this will require co-operation between a wide range of professionals in the mundane application of programme, system development and application disciplines, which will be novel to most.

Wherever possible, solutions should be developed from existing viable and sustainable systems. For example, the desirability of a common reference number in the correlation of all interactions between medical professionals and patients can be achieved simply by treating the patients' NHS number (currently held on the National Strategic Tracing Service) as a Unique Reference Number (URN).

The endgame - A vision of success

A vision of success for 2005 would include the following:

- Accurate and up-to-date patient information being available to those needing to make clinical judgements in the right format, for the right patient, at the right place and time.
- Sharing of patients' medical information between healthcare professionals in hospitals and in general practice, with subsets available to those (e.g. paramedics) who may need to give emergency care.
- Protection of an individual's data records, with access controlled in accordance with informed patient consent and recorded by audit trail, with policing routines in which both public and professionals have confidence.
- Duties of confidentiality enshrined in good practice codes which replace inflexible barriers to sharing data so as to balance the need for rapid access to accurate data against patients' rights to confidentiality.

The main challenges to the achievement of this vision are not technical, but cultural, institutional, managerial and political and the immediate need is to inform Parliamentarians, medical interest groups and political think-tanks of the issues that need to be resolved, with clear public support, in order to achieve success.

In moving forward here, it will be important to distinguish between responsibility for *accuracy and validity* of information, and responsibility for *ensuring availability* of information. Equally important will be to distinguish between information that is essential for effective medical treatment and that which may be in a patient record for other purposes.

Conclusion and Recommendations

At this stage in its deliberations, the working group welcomes further input but in order to stimulate focused response has chosen to offer for comment a number of recommendations as follows:

We recommend that:

1. A central index of permissions be collected from patients at a convenient time, e.g. registration, in the form of a generic permissions pro-forma.
2. Citizens are given the ability to help manage the use of their personal data records.
3. All involved in medical records are given clear guidance as to what information can and should be made available to whom, under what circumstances and what should not.
4. Those responsible for NHS policy and implementation enlist the informed support and consent of healthcare professionals and patients (including politicians at all levels), as well as of suppliers of systems and services, in setting realistic and trusted frameworks within which practical progress can be made.
5. The roles, responsibilities and obligations of staff be clearly set out, especially where medical data is exchanged across organisational boundaries and/or with those responsible for providing community care.
6. A step-by-step approach is adopted for developing, testing and piloting new systems with potential for large-scale roll-out and interoperability within an overarching strategic framework.

These principles, however, will need to be considered in a wider context and there is also a need for consultative workshops to look at:

- Relationships between the custodians, producers, owners and consumers of the personal and other information (not just medical) related to health care and social welfare and the legal and ethical obligations and rights of health care professionals, researchers, care and social workers, administrative staff and patients with regard to knowledge management.
- Processes (including those enabled by new technologies) to support adherence to relevant legislation, regulations and good practice regarding capture, storage, disclosure, amendment, destruction and quality management of information. These include the provision of authentication routines and audit trails to allow the rapid validation of requests to access controlled information (knowledge management).