CONFIDENTIALITY AND SECURITY ISSUES SURROUNDING CLINICAL INFORMATION MANAGEMENT

Roy McClelland
Confidentiality Advisory Group
Royal College of Psychiatrists

Introduction

“Security holds the Key” was the title of a recent Sunday Times article concerned with e-commerce. However it applies just as readily to the health sector. The need, indeed the requirement, to safeguard the confidentiality of information that patients share with clinicians is as fundamental as the principal of consent. This issue has come to the fore in the context of the rapid developments in applications of information and communication technologies within society in general and within the health sector in particular. There are also changing societal expectations regarding access to information, to confidentiality and to disclosure. The emerging scenarios present significant challenges in relation to the traditional methods used to deal with the privacy and confidentiality of personal information.

There is however at core a tension between the needs for patient information to optimise the quality of care and the expectation of patients that information about them will be kept confidential. As the Caldicott Report notes, balancing such potential conflicts requires the development of and adherence to explicit and transparent principles of good practice on all aspects of patient identifiable information (Caldicott Report 1997). Within this context there is a need to establish a new culture for handling healthcare information – a culture that recognises, understands and responds to the changing structure of healthcare and healthcare delivery systems which depend increasingly upon the ready sharing and manipulation of patient information (France 1997).

As Chairman of the College’s Confidentiality Advisory Group I regularly receive correspondence from clinicians, managers and solicitors seeking advice on decisions in relation to Clinical Information Management. It is my impression that for most of us there is a
considerable ignorance on our duties and obligations in relation to confidentiality and its boundaries, for example:

- our obligations to ensure that patients are informed of just how their confidential information is used,
- the use of research databases,
- the disclosure of patient identifiable information outside the health service.

**Ethical Principles**

Confidentiality considered from a duty perspective is grounded in the principle of respect for autonomy – doctors explicitly or implicitly promise their patients that they will keep confidential the information provided to them – keeping promises is a way of respecting autonomy. There are consequentialist arguments supporting keeping of confidence, for without promises of confidentiality patients are far less likely to share the private and sensitive information required for their care.

However the duty of confidentiality exists within a wider social context in which other moral obligations may compete. These competing appeals set limits to medical confidentiality. Doctors therefore have a further duty to their patients – to inform them that in exceptional defined circumstances (usually harm to others) the duty of confidentiality may be overridden.

**Legal Basis**

Confidentiality and privacy are also legal concepts and the relationship between healthcare professionals and their patients carries with it legal obligations of confidence as well as ethical ones.

The Human Rights Act (1998) allows individuals for the first time to pursue claims in UK court. Convention grounds may now be invoked in proceedings for established torts such as breach of confidence or to bring an action against a public authority on the basis of the Convention’s right to privacy under Article 8. The Human Rights Act underpins other legislation concerned with confidentiality – but further, public authorities are required to
construe the legislation under which they operate in accordance with the European Convention on Human Rights and to ensure that their actions and those of their staff are consistent with it. The Data Protection Act (1998) gives effect in UK law to EC directive 95/46/EC and introduces 8 data protection principles that set out standards of information processing or handling. The term “processing” includes the collection, use and disclosure of personal data. The DPA 98 is now a central plank in the statutory framework underpinning confidentiality in Clinical Information Management. The information Commissioner has issued guidance on the applications of the Act in relation to the use and disclosure of health data (The Data Protection Act 1998 – Legal Guidance) “www.informationcommissioner.gov.uk.”

The first data protection principle states that “personal data shall be processed fairly, lawfully and shall not be processed unless at least one of the conditions in Schedule 2 is met and in the case of sensitive personal data at least one of the conditions in Schedule 3 is also met”. That is there are three cumulative requirements of this principle:

- the requirement to satisfy a condition in Schedule 2 and Schedule 3;
- the requirement to collect personal information fairly;
- the requirement to process personal information lawfully.

**Schedules 2 and 3.** In practice it is unlikely to be difficult to satisfy the conditions of Schedule 2 and 3. At core Schedule 2 requires that processing (use) is **necessary** for the exercise of functions of a public nature exercised in the public interest by any person. Schedule 3 requires that processing is with the consent of the data subject, or that “the processing is necessary for medical purposes and is undertaken by a health professional (or a person owing a duty of confidentiality equivalent to that owed by a health professional”). The term “medical purposes” embraces preventative medicine, medical diagnosis, medical research, the provision of care and treatment, the management of healthcare services.

The Necessity Test. Many of the conditions for processing set out in Schedules 2 and 3 specify that the processing must be “necessary” for the purpose stated. In order to satisfy one of the conditions other than processing with consent, data controllers (doctors frequently) must be able to show that it will not be possible to achieve their purposes with a reasonable degree of ease without the processing of “personal” data. The Commissioner takes the view that when
considering the issue of necessity, data controllers must consider objectively whether: such purposes can be achieved only by the processing of personal data and the processing is proportioned to the aim pursued.

**The requirement to collect personal data fairly.** There is an obligation on data controllers (doctors) to provide certain information to data subjects when collect their personal data. This information is often referred to as “fair processing information”. We should ensure that our patients are provided with the relevant information indicating the purpose or purposes for which their clinical information is typically used. Information is required as to what information is being used. For example patients are likely to expect that basic information will be recorded as to the diagnosis and treatment. They may however by surprised to find that other information has been recorded, for example the circumstances surrounding an injury.

(i) Patients require information as to specific disclosures. Given the sensitivity of medical information a patient should be informed of any non-routine disclosures of their information.

(ii) Patients must be given information as to whether any secondary uses or disclosures are optional. Where patients have a choice these choices should be brought to their attention.

(iii) Timing. When should fair processing information be provided? An obvious point at which patients should be provided with information is at the onset of an episode of care (IC). It is good practice to remind patients of this information from time to time (IC). The Commissioner points out that patients who will have their personal data processed for additional purposes will need to be provided with this further information in order to satisfy “the fair processing” requirements.

(iv) How should the fair processing information be given? The Information Commissioner suggests that such information may be provided: as a standard information leaflet, face to face in the course of a consultant, included within an appointment letter from a hospital or clinic. The effort involved in providing this information can be minimised by integrating the process with existing procedures.
The requirement to process personal data lawfully. While the DPA does not provide any guidance on the meaning of the term “lawful” the principle means that the data controller must comply with all relevant rules of law whether derived from statute or common law. While there are potentially a large number of considerations which data controllers processing health data must take, the practice the key issue in this context is likely to be the common law duty of confidence (Guidance page 15). Duty of Confidence is a common law concept rather than a statutory requirement and as such it derives from cases that have been considered by the courts. Indeed it is the Commissioner’s assumption that the processing of health data by a health professional is subject to a duty of confidence even though explicit consent for processing is not a requirement of Schedules 2 and 3 – based essentially on case law.

Guidance. In addition to laws, statutory and case law, there are a number of sources of guidance:

General Medical Council (2000) Confidentiality: Protecting and Providing Information; (www.gmc-uk.org)
Information Commissioner (2002): use and disclosure of health data, guidance on the application of the Data Protection Act 1998; (www.informationcommissioner.gov.uk)

Royal College of Psychiatrists (2000) Good Psychiatric Practice: Confidentiality. (www.rcpsych.ac.uk)

Disclosure – Confidentiality Exceptions.

Patient information is generally held under ethical and legal obligations of confidentiality. The courts have recognised three exceptions to the Duty of Confidence:

Where the individual to whom the information relates has consented;
Where there is need a legal compulsion;
Where there is an over-riding duty to the public.

Where there is a duty defined by an Act of Parliament. In a small number of particular circumstances a doctor has a statutory responsibility to disclose to the relevant authorities. For example the Public Health (Infectious Diseases) Regulations 1988; the Road Traffic Act 1988;
there are also obligations to pass on information under the Mental Health Act 1983; The Childrens Act, Crime and Disorder Act 1998 (S115), (Criminal Justice Bill) allow doctors to disclose under appropriate circumstances, they do not require doctors to disclose, i.e. justification rather than obligation.

More recently s60 of the Health and Social Care Act 2001 creates a power for the Secretary of State to make orders requiring the disclosure of patient data that would otherwise be prevented by a duty of confidence. This is intended essentially as a temporary measure until anonymisation measures or appropriate recording of consent can be put in place for some secondary uses. A major stimulus is the requirements of registries, particularly cancer registries. An independent statutory Patient Information Advisory Group oversees all applications for exemptions from the duty of confidence to use patient identifiable information. The first regulations to be made under Section 60 of the Act are the Health Service (Control of Patient Information) Regulations 2002 to support the operation of cancer registries and Public Health Laboratory Services in respect of communicable diseases and other risks to public health.

**Consent.** Most uses (primary or secondary) or disclosures of healthcare information will be justified by having obtained the consent of a patient. Information provided in confidence should not be used (primary or secondary use) or disclosed in a form that might identify a patient, without his/her consent.

As the Commissioner notes there are three key conditions that must be satisfied for consent to be effective. First it is must be informed. A patient cannot be deemed to have consented to something of which he/she is ignorant. It is extremely important that patients are made aware of the information sharing that must take place in order to provide them with appropriate care including the requirements of Clinical Governance and clinical audits (fair processing information - note what, when, how above.)  Second the person giving consent must have some degree of choice. Thirdly there must be some indication that the patient has given consent – this may be expressed (explicit) or implied. As the Commissioner notes it is a mistake to assume that implied consent is less valid than expressed consent. However both must be equally informed.
Primary Uses. Where patients have been informed of the use and sharing of their information and the choice that they have, then expressed consent is not usually needed for information sharing needed to provide healthcare.

Secondary Uses. Many current uses of confidential patient information however do not contribute to or support the healthcare that a patient receives. We cannot assume patients seeking healthcare are content for their information to be used in these ways. Patients have the right to object to the use or sharing of confidential information that identifies them. Patients need to be made aware of this right. It is wrong to assume consent. Additional efforts to gain consent are required. Alternatively approaches that do no rely on confidential and identifiable information should be adopted.

The GMC Guidance is quite explicit: “Disclosure of information about patients for purposes such as epidemiology, public health safety, or the administration of health services, or for the use in education and training, clinical or medical audit, or research, is unlikely to have personal consequences for the patient. In these circumstances you should still obtain patients’ expressed consent to use of identifiable data or arrange for members of the healthcare team to anonymise records”. The guidance also states that where information is needed and where it is not practicable to obtain expressed consent or to anonymise records, information may still be disclosed providing such disclosure is kept to a minimum and you are satisfied that patients have been informed or have access to information that they have a right to object that their objection will be respected.

Duty to the Public - Disclosure outside the NHS. Disclosure of confidential information to third parties outside the NHS may be justifiable in the public interest on the basis of the benefits it brings and the harms averted by disclosure. Where failure to disclose information may expose others to risk of death or serious harm and there is a high probability that disclosure of information would lead to a reduction in that risk, then disclosure would be justified. Disclosure may also be justified where it may assist in the prevention, detection or prosecution of serious crime.

There is in civil law no general duty to prevent a third party from causing damage to another. However, a duty of care may be owed if there is “proximity” between one’s patient and a potential victim where the latter is “identifiable” or “identified” (Court of Appeal re: Palmer v West Tees Health Authority (1999).
Each case must be considered on its merits – the test being whether the release of information to protect the public interest (which includes protecting members of the public) prevails over the duty of confidence to the patient (ethical test) or the public interest in maintaining confidence (legal test). Decisions to disclose patient identifiable information outside the NHS, apart from the few statutory exceptions, are matters of judgement – judgements that may be finally balanced. Such balancing would need to take into account the various legal responsibilities at stake, including the duty of confidence to the individual, and the public interest in the health service maintaining confidence. Consideration will need to be given as to whether the harm that could result from disclosure (eg the possible damage to the relationship of trust or the likelihood of non-compliance with a programme of healthcare intervention in the future) is likely to be outweighed by the positive benefit. The potential benefit would need to be soundly grounded on the expectation that disclosure would have the desired effect.

We should note that many of these situations will require good communication and support to be available for patients whose confidentiality is to be breached. Whether a breach of confidence is justifiable in the public interest will depend to some extent on the scope of disclosure. Therefore when considering whether to disclose, the psychiatrist should also consider the extent of the information to disclose and to whom it is appropriate to disclose such information (minimalist approach – the College position).

Ultimately a court would take careful account of the opinion of fellow doctors on the guidance of professional organisations as to whether a decision concerning disclosure was within the reasonable practice of a responsible body of medical practitioners (Royal College of Psychiatrists Good Psychiatric Practice: Confidentiality (CR85). We are however facing a moving target and the College’s Advisory Group on Confidentiality aims at providing an ongoing source of advice to the College and its members.