

World Data Protection Report

International Information for International Businesses

Monthly news and analysis of data protection and privacy issues from around the world

Electronic health records: data protection issues in Europe

*By Clare Sellars and Dr Amanda Easey
IPM&T Group, McDermott Will & Emery UK LLP*

*This article has been published in the April 2008 issue of
BNAI's World Data Protection Report*



www.bnai.com

Personal Data

Europe and United Kingdom

Electronic health records: data protection issues in Europe

Written by Clare Sellars, Counsel,

csellars@europe.mwe.com and

Dr Amanda Easey, Associate, aeasey@europe.mwe.com,

IPM&T Group, McDermott Will & Emery UK LLP

The eHealth industry in Europe is undoubtedly at an exciting stage of its development. As a result of this, it is increasingly becoming a focus of attention for the European Commission, (the 'Commission'), as demonstrated by the Commission's recent paper, *Accelerating the Development of the eHealth Market in Europe*¹, which recognises the potential economic and social value of the eHealth market and the opportunities for European (and other) companies in this sector to become global leaders in this field.

The Commission also recently proposed a *Lead Market Initiative* for the European eHealth market, which aims to work with industry to determine a 'road map' and remove barriers to development in this area. The eHealth market is identified as critical to the development of a single European market and the Commission has confirmed its commitment to the development of this sector in Europe, estimated to be worth approximately €21bn in 2006. The initiative sets out various policy recommendations aimed to encourage the development of the eHealth market by improving legal certainty in various areas including, in particular, privacy and personal data. The application of personal data protection legislation to eHealth tools and services is highlighted as an area needing special attention to ensure that the development of the European eHealth market is not impeded.

Data protection issues were also a focus of *Legally eHealth* – the European Commission's study on the legal and regulatory aspects of eHealth. This recommended the adoption of a directive or a code of conduct to provide greater legal certainty in respect of the requirements for the processing of personal data and the protection of privacy in the eHealth sector.

Electronic health records

One aspect of European eHealth expansion is the increasing drive to store personal health information in electronic form, as electronic health records, ('EHRs'). A number of data protection and privacy issues can arise in the implementation and operation of EHR systems. Within the U.K., the National Health Service, ('NHS') Care Records Service, (the 'NHS CRS'), (which is currently being established), provides an excellent example of the various data protection and privacy challenges associated with EHR systems.

Although the NHS CRS is being established in the context of a national health service provided by an E.U. Member State, the issues which it raises apply more broadly in the context of

both public and privately provided health services and so should be of interest to those involved in the provision within Europe of national health care systems and private healthcare alike. Once implemented, the NHS CRS will hold the health records of the majority of U.K. citizens. The practicalities of installing and running a database of sensitive, health related personal data on this scale has already raised some interesting data protection considerations, which are discussed in more detail below.

Potential benefits

Proponents of EHRs argue that paper medical records systems can compromise patient care. In the case of the U.K.'s NHS, multiple sets of paper and electronic records for individual patients have historically been held at several sites depending on where the patient has accessed care, with no rapid system of cross-referencing or integration of such records being available. This lack of an integrated records system can result in communication delays between NHS staff, which can affect the speed of care to patients, especially those with complex health problems. The tragic case in 2007 of repeated misdiagnoses leading to the death of a woman who was seen by eight different general practitioners ('GPs') who were unable to access each other's paper records over a public holiday weekend illustrates this. There is clearly a need for health professionals to have access to complete, up-to-date, integrated, rapidly accessible and cross-referenced data about their patients in order to be able to provide the highest quality of care.

EHRs should also bring cost benefits as, for example, duplication of laboratory and radiological examinations as a result of lost or unavailable reports should be avoided.

Potential risks

There are, however, data protection issues which arise from the recording of personal information in an electronic record. Electronic systems make confidential data more easily and rapidly accessible to a wider circle of recipients than paper systems, with an associated greater potential for breaches of confidentiality.

The public are becoming increasingly aware of the risks of identity theft and the need for data security. In addition to the loss of computer disks containing personal information in the past by government departments, there have been several reports of thefts and losses of mobile devices and storage media, such as laptop computers and USB drives containing the medical details of NHS patients. A recent report stated that at least nine NHS trusts have lost patient information. In April 2007, inadequate security on the NHS Medical Training Application Service, website allowed members of the public to access certain personal information of junior doctors,

including telephone numbers, addresses and also some sensitive personal data including details of previous convictions and sexual orientation. The Information Commissioner's Office has recently stated that this breach of security was in breach of the Data Protection Act 1998 ('DPA'), for which the Department of Health could potentially face prosecution.

Such security breaches are being treated very seriously. It was recently reported that the chief executive of the NHS has instructed all NHS trust chief executives to check security arrangements for laptops, CDs and USB pen drives and review their data transfer arrangements. In November 2007, the Information Commissioner suggested to the House of Lords Constitution Committee inquiry on surveillance and data protection that health professionals who are grossly negligent in failing to ensure that patient information is protected, for example by leaving a laptop containing unencrypted patient information in a place where it is stolen, should be prosecuted for breach of the DPA. Currently, there are no legal provisions for medical staff to be fined by the court in these circumstances, but the Information Commissioner has proposed that fines should be introduced, which could be unlimited if imposed by a Crown Court. A spokesman for the General Medical Council (the 'GMC'), the professional regulatory body for doctors in the U.K., stated to the same committee that doctors who seriously and persistently breach data protection guidance published by the GMC may have their registration status reviewed, with the possibility of being struck off the medical register.

Concern about data protection is not exclusive to patients: a recent survey for the Times newspaper found that 80 percent of doctors were concerned that a central database of patient health records would be insecure.

There is, therefore, a conflict between the need for comprehensive, accessible patient data and the data protection rights of individuals. Unfortunately, press reports of data losses from devices such as laptops, USB sticks and CDs undermines patient confidence that their personal data is being used and stored appropriately by healthcare professionals. If this erosion of trust results in individuals being unwilling to provide personal information to health professionals involved in their care, resulting in incomplete medical records, this could negatively affect their quality of health care.

The legal framework for data protection in the U.K.

Personal data recorded in an EHR must be collected, held and processed in accordance with the DPA, which implements the Data Protection Directive 95/46/EC, (the 'Directive') in the U.K.

The DPA applies to all 'data controllers' who collect, hold and or process personal data of data subjects (in this case patients). For the purposes of the Act, a 'data controller' is a person who either alone or jointly in common with others determines the purposes for which and the manner in which any personal data are, or are to be, processed.

What is personal data?

Personal data is defined in the DPA as 'data which relate to a living individual who can be identified: (a) from those data; or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller'.

The DPA also defines 'sensitive personal data'. Sensitive personal data include certain categories of data which are likely to be regarded as especially private by the data subjects to whom they relate, for example, personal information as to physical or mental health or condition, racial and ethnic origin, religious beliefs and sexual life. Such data are subject to additional safeguards. Clearly, much information included in patient health records are likely to comprise sensitive personal data. In addition to information relating specifically to a person's health, medical records may routinely contain other personal and social information that the medical practitioner creating or updating the record considers relevant, such as living arrangements, occupation, racial or ethnic origin, sexuality and sexual history, and religious beliefs. This information may be relevant to an aspect of a patient's care and therefore may be recorded by a health professional under the DPA if 'necessary for medical purposes'.

The data protection principles

In the U.K., personal data may only be processed in accordance with eight data protection principles which are set out in the DPA. These principles include, among other things, the need to process data fairly and lawfully, to only obtain data for specified and lawful purposes, to ensure that data is adequate, accurate, up-to-date, relevant and not excessive, to ensure that data is not kept longer than necessary, to ensure that data is not transferred outside of the European Economic Area, (the 'EEA') unless an adequate level of protection in the country to which the data is transferred has been ensured, and to ensure that data is secure and protected against accidental loss or damage.

The first data protection principle

In order to process personal data fairly and lawfully in accordance with the first data protection principle at least one of a series of conditions (see Schedule 2 of the DPA) must be satisfied. The conditions most likely to be satisfied in respect of health related data include:

- processing with the consent of the data subject (the patient to whom the data relates);
- processing which is necessary to protect the data subjects' vital interests;
- processing which is necessary for the exercise of functions of a public nature exercised in the public interest by any person; and
- processing which is necessary for the purposes of the legitimate interests pursued by the data controller or those of a third party to whom the data are disclosed, except where the processing is prejudicial to the rights and freedoms or legitimate interests of the data subjects.

As noted above, sensitive personal data are subject to additional safeguards and may only be processed if at least one of a further set of conditions are also satisfied. The conditions which are most likely to be satisfied in respect of health related data include:

- processing with the explicit consent of the data subject;

- processing necessary to protect the vital interests of the data subject, or another person where it is not possible to get consent;
- processing necessary for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings), obtaining legal advice, or otherwise necessary for the purpose of establishing, exercising or defending legal rights;
- processing which 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. 'Medical purposes' include preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services. The definition of health professional includes dentists, pharmacists, opticians, osteopaths and chiropractors; a variety of professions may therefore legally process patient information for medical purposes;
- processing of medical data or data relating to ethnic origin for monitoring purposes; and
- processing in the substantial public interest, necessary for the purpose of research the aim of which is not to support decisions with respect to any particular data subject otherwise than with the explicit consent of the data subject and which is not likely to cause substantial damage/distress to the data subject or any other person.

Fair processing code

The DPA requires data controllers to provide certain information to patients, known as the 'fair processing code', when collecting their personal data (whether for the purposes of creating or amending EHRs or otherwise). This information includes the data controller's identity, the identity of any representative of the data controller nominated for the purposes of the DPA, the purpose(s) for which the data are to be processed and any further information which is necessary taking into account the specific circumstances in which the data are or are to be processed to allow the processing in respect of the patient to be fair. Information regarding the identity of the data controller and the purposes for which the data are to be processed need to be reasonably specific. Patients should also be informed about what data have been or are to be recorded if this is unclear. Patients also need to know whether any secondary uses or disclosures of data are optional and if they have a choice regarding the provision of information, disclosure of it to third parties, or the right to object to certain uses or disclosures.

Lawful processing – data protection and the common law duty of confidence

One issue that requires careful consideration by NHS entities and also by service providers to the NHS which are holding and processing NHS patient records is the interaction between the DPA and the common law duty of confidence and ensuring that legal obligations in both these respects have been complied with.

As noted above, the first data protection principle provides that personal data must be processed fairly and lawfully and must be processed in accordance with at least one of the conditions in Schedule 2 to the DPA. Where the data being

processed comprise sensitive personal data (e.g. information concerning the physical/mental health of data subjects) it must also be processed in accordance with at least one of the conditions in Schedule 3 of the DPA.

To ensure that the fair and lawful processing requirements are complied with, NHS guidance stresses that personal data must be processed in accordance with all relevant laws including, without limitation, the common law duty of confidence. Although the DPA does not require that the explicit consent of data subjects must be obtained in order to process health related information, compliance with the 'lawful' requirement of the first data protection principle included in the DPA means that the common law duty of confidence must be considered. The common law duty of confidence provides that information given in confidence must not be disclosed without the consent of the provider of the information. Effectively, this means that when health information is provided to someone outside of a patient's care team the data subject's consent to such processing will be necessary and in many cases there will be an implied requirement to obtain patient consent for the processing of data, as to process without consent would amount to a breach of confidence, which would lead to a breach of the requirement to process personal data lawfully under the DPA.

NHS entities and private providers alike who are acting as data controllers in respect of personal data of NHS patients should consider this issue carefully in respect of the collecting, holding and processing of personal data of patients in the context of EHR systems to determine whether consent to processing of EHRs is necessary in any particular context and, if so, whether all relevant patient consents have been obtained.

Other issues

Other difficulties may also arise in respect of EHRs from a data protection viewpoint, for instance, where personal data is recorded routinely for purposes which are not clearly medical, or where access to the information is available to any health professional responsible for that patient with no consideration of whether the information is relevant to the type of care being provided. In these circumstances, the processing of such personal and social information may be considered to be excessive in relation to the purpose for which the data was processed, and therefore may be in breach of the DPA.

The NHS CRS

The NHS CRS comprises a national broadband network linking all NHS sites which will provide the structure for access to the EHRs of all NHS patients. It is intended that there will be a single central national system of EHRs, called the national data spine, with the functionality for local IT systems to link in to it. The Information Commissioner has stated that the NHS must comply with the DPA in implementing the NHS CRS and is monitoring the implementation and operation of the service. Initially, care records will contain limited details such as the individual's drug history, allergies and adverse drug reactions, comprising a 'Summary Care Record'. Over time, more detailed health records will be linked between local organisations such as hospitals, clinics and GPs.

Security

As noted above, the DPA requires that personal data must be protected against unauthorised or unlawful processing or accidental loss or damage by 'appropriate technical and organisational measures'. When the NHS CRS is fully implemented, it is anticipated that the NHS broadband network will be protected from attack by hackers by multiple security measures including firewalls and intrusion detection systems. It is also intended that the NHS CRS will include a series of access controls for NHS employees accessing the database at their place of work which will include:

- the use of a unique identifying reference for each patient (the NHS number);
- registration of all users with a central authority to obtain a smartcard and a passcode (chip and pin). Strict prohibitions on the sharing of access cards and passwords will be introduced;
- access to the system will only be permitted where there is a 'legitimate relationship' between the system user and the patient. Staff accessing patient records should be registered on the system as working in a team providing care to the relevant patients;
- each registered user will have 'role based' access which defines the extent to which information can be accessed and amended. Staff will only be able to access as much information as is needed for the purpose of their role, for example, a clinic clerk may only have access to administrative information;
- a system of 'sealed envelopes' permitting partial access to information for the majority of users will be introduced. More sensitive information is 'sealed' and only accessible to the care team which created the information;
- the system will include an audit trail whereby records are kept of all instances of access to a patient's care record, with alerts triggered when access is not justifiable. Specific individuals will be responsible for reviewing such alerts and taking appropriate action; and
- appropriate training on the permitted use of patient information and the relevant requirements of data protection law will be provided to system users.

Other possible safeguards include screensavers and 'time-out' periods if the user does not log out of the system properly, removal of links to other networks (for example, internet access) and locating computer screens or other access devices in areas to which the general public do not have access.

Practical issues

Ultimately, the effectiveness of such controls will be reliant on the compliance of the system users. Although strict access control is necessary to protect the data protection rights of individuals whose personal data has been recorded on a central database, some practical issues which should be considered are set out below.

Security of mobile data storage devices

Medical staff are increasingly using mobile data storage devices such as USB pen drives to hand over patient information to other team members at the end of a shift. Such data may not be encrypted and small devices may more easily be lost or stolen. In addition, they may contain duplicate or additional information to that on the central database. A strict policy either banning the use of such devices and requiring all information to be inputted to the central database, or requiring all information on these devices to be securely encrypted is recommended. Such a policy should also apply to patient information stored on laptops, or on the desktop of computers kept in public areas. Staff should also be made aware that their professional registration may be at risk if data security is breached due to their negligence.

Temporary and locum staff

Consideration should be given to the issue of how access to the system will be provided to such staff immediately. Such staff may be employed at short notice and arrive on site outside of the normal working hours of the human resources or IT departments. This problem could be resolved by the provision of temporary smartcards and passcodes however, the use and location of temporary cards would need to be strictly monitored as they would render the NHS CRS especially vulnerable to abuse and the current holder of the card would need to be registered at all times in order to ensure an effective audit trail of access. Temporary employees would also need to be registered as having a 'legitimate relationship' to patients in order to be able to access the system.

Creation of new 'legitimate relationships'

Where a patient is referred to another health professional such referrals are often made orally and access to patient information may be required at short notice. If the health professional is unable to register a new legitimate relationship on behalf of their colleague, will their colleague's access to that information be limited? If health professionals do not have the authority to register a legitimate relationship, who will? And will this facility be available at all times? Conversely, how will the continued legitimacy of relationships be monitored and updated over time, for example where patient care is handed over between medical teams? Will an EHR permit an ever-increasing number of 'legitimate relationships' which may reduce the security of the data by permitting staff who are no longer responsible for the care of a patient to access that patient's data? Appropriate security measures should therefore include the prevention of access to the system of staff with outdated legitimate relationships.

Who will input data to the system?

Clinicians will require the facility to delegate the input of detailed information to administrative staff. Such staff will need to be subject to an obligation of secrecy equivalent to that of the clinician. There are already anecdotal reports of administrative staff being provided with extended access rights to EHRs as a matter of convenience. Under the provisions of the DPA, persons processing personal data must be required, by contract, to only deal with that data

according to the instructions of the data controller, and to appropriately ensure the security of that data. The employment contracts of administrative staff should therefore contain appropriate data protection related provisions.

Access to the NHS CRS for purposes allied to medicine

It is likely that, in future, access to the NHS CRS will be available to individuals and organisations outside the NHS, such as counsellors, social workers, pharmacists and dentists.² If such access extends the purposes for which a patient's personal data can be used beyond the purposes in respect of which the patient gave express or implied consent to the use of such data, such access must be notified to the patient and, in some cases, the patient's consent must be obtained to ensure that the processing of the patient's data is lawful (see above).

Any non-NHS employee granted access to the NHS CRS must be subject to the same obligations of confidentiality and security as an NHS employee. The issue of monitoring compliance with such obligations must be considered, along with the procedures to be followed in the event of breach.

Sealed records

The management of sealed records may inadvertently reveal patient information. The mere fact that information is flagged as not being accessible indicates that highly sensitive information exists for that patient, which is a piece of personal data in itself. The degree to which information is veiled should also be considered, for example, a record of appointments with a particular consultant or clinic may reveal sensitive information even if the diagnosis and clinic notes are veiled. One option would be to 'seal and lock' the information so that no flag exists to show information is missing. This may create, however, a conflict between the individual's data protection rights and the NHS's duty of care to ensure relevant patient information is available between health professionals. If information cannot be 'unsealed' in emergency situations, patient safety and continuity of care may be compromised.

Contemporaneous input of data

To be effective the NHS CRS will need to contain up-to-date information. With paper records, patient information can be recorded by the bedside. Ideally, information should be inputted directly to the NHS CRS, either through a computer terminal at the bedside or a mobile device connected to the system. If this facility is not available, clinicians will be likely to continue to use paper records in parallel with the EHR which will increase administrative burden and may compromise patient safety if information is not inputted in a timely way. As a related point, data input devices will need to be fit for use in a clinical environment and be compliant with infection control policies. The Government plans to 'deep clean' every NHS ward, including the cleaning of IT equipment.

Access for mobile healthcare workers

Some individuals requiring access are mobile between and outside of NHS sites, e.g. clinics at different hospitals or

paramedics and community nurses. Consideration as to how this access will be managed will be necessary.

Employees processing patient data

All parties with access to EHRs need to understand their legal and professional obligations when handling sensitive personal data. Data controllers must ensure that employees and agents processing personal data on their behalf are reliable and trustworthy. Under the seventh principle of the DPA, security guarantees from data processors must be imposed contractually and made or evidenced in writing. Staff obligations should therefore be set out in employment contracts, staff handbooks and policies, and job descriptions should define the security responsibilities of the post. Ideally, employment contracts should include undertakings not to disclose confidential information; if they do not, separate confidentiality agreements will be necessary. As discussed, different levels of security control should exist depending on the sensitivity of the data; data processors should be aware of the permissible degree of access for their particular role and understand what is 'confidential information'. Contracts with agencies for locum staff should explicitly contain these obligations in writing.

Staff should be made aware of disciplinary measures which may be imposed in the event of a breach of their legal obligations or their employer's security policy. In particular, clear policies should be implemented regarding the security of mobile devices, for example, requiring that equipment is not left in cars, is virus checked regularly and cannot connect to other networks with which information might be exchanged.

One way to ensure that data processors have been adequately informed about their obligations would be to require training before smartcards and passcodes are issued, although this might cause difficulties for agency and locum staff employed at short notice if training did not take place immediately before their period of work commenced.

Procedures should be implemented regarding departing staff. Smartcards should be retained and passcodes changed promptly. Obsolete names should be removed from user lists.

Conclusion

The potential benefits offered by EHR systems of delivering faster and more efficient patient care at lower long-term cost are undoubtedly considerable and attractive however, these benefits cannot be realised at the expense of the protection of personal data of patients. The implementation of the NHS CRS provides a good illustration of some of the data protection challenges created by EHRs, but also offers useful food for thought regarding the ways in which such challenges can be overcome. Regardless of the data protection issues which are raised, there can be no doubt that EHRs are here to stay in Europe, both in the context of state run health care systems and private healthcare.

1 eHealth Taskforce report December 2007

2 NHS Connecting for Health: Guidance for the NHS about accessing patient information in new and different ways and what this means for confidentiality, December 22, 2006.