SCRIPT-ed

Volume 4, Issue 1, March 2007

An Electronic Health Record for Scotland: Legal Problems Regarding Access and Maintenance

Dr Renate Gertz[*]

Abstract

This paper examines the problems of confidentiality and liability in the new Scottish an Electronic Health Record (EHR) from two perspectives, firstly, a question of creation and control over the EHR, and second, a problem of access to the EHR.

DOI: 10.2966/scrip.040107.152

[*] Research Fellow, AHRC Centre for Studies in Intellectual Property and Technology Law, School of Law and Centre for International Public Health Policy, University of Edinburgh.

1. Introduction

Scotland intends to introduce an Electronic Health Record (EHR) in the near future to provide an open data system throughout the health service to improve access to a current health record and to prevent the so-called 'multiple-blood-test-syndrome' due to lack of communication between health care providers – sometimes even within the same hospital. This vision, however, is accompanied by various legal and ethical problems. Whilst offering potential advantages in terms of increased efficiency with in the healthcare system and reducing burdens on patients, this paper examines the problems of confidentiality and liability in two different aspects, regarding, first, a question of creation and control over the EHR, and second, a problem of access to the EHR.

2. Record creation and control

The first issue to be examined is the question of the creation of and control over the EHR. This includes examining who will need to be responsible for maintaining the record and adding information and the potential effects this may have on liability.

2.1. Four models for an EHR

Terry and Francis have suggested four types of models for an EHR[1]:

1. The Personal EHR model focuses on the patient as the chief manager and custodian of the record, which is composed of fields into which the patient enters the relevant data or manages the data export from the GP's records.
2. The Shared EHR model sees responsibility for maintenance and control shared between patient and GP. Responsibility can shift from resting on both patient and GP to a fairly one-sided arrangement with either party being more responsible for maintenance and control over the record.
3. For the Trustee model, patients enter into a contract with a third party, the trustee, to keep and control the EHR. Overall control, however, will still rest with the patient.
4. Finally, the Interoperable EHR model constitutes a fully longitudinal system, transforming the current paper records system to its electronic equivalent. This can be operated at either regional or national level with no patient involvement. Hence, patients will not have any control over this type of record.

[1] See Terry, N. and Francis, L.P., "Ensuring the privacy and confidentiality of EHRs," *University of Illinois Law Review* (Forthcoming 2007)

2.1.1. Confidentiality issues

Obviously, a record managed and controlled by the patient will create less confidentiality problems, as it is the patient him/herself that will determine access to the information. Still, patients might approve access to the record without appreciating the wider privacy implications. In the shared record, it will depend on where the responsibility for maintaining and controlling the record will ultimately lie. The more patient involvement, the less confidentiality and data protection problems can be expected. In the trustee model, confidentiality is secured as the patient decides what data will be transferred to the fiduciary. There is, however, the possibility for the trustee to break the contract and process data though unauthorised to do so. Hence, the degree of maintaining confidentiality will depend on the trustworthiness of the fiduciary. The final model will be the one carrying the greatest risk of breaches of confidentiality and/or data protection with little or no patient involvement, as sharing of data in a legally and ethically sound way will fall solely within the responsibility of the health care providers. Without a stringent and enforceable access policy in place, unauthorised staff members of the healthcare provider may have access to sensitive personal data. With proper systems having been instituted, however, this could also be the most protected system.

2.1.2. Liability issues

In the current paper-based system, if an error in the medical records leads to a negative development in the patient's health, the healthcare professionals responsible for the entry into the records and the subsequent treatment will be held liable – no matter whether they are one and same or different persons. A larger patient involvement in creating and controlling the record may shift this liability.

The UK courts have developed a complex mechanism to determine liability for healthcare. The main requirement for liability is that negligence must be proven,[2] with three requirements: the healthcare professional owes the patient a duty of care; a breach of this duty has occurred, meaning that the standard of treatment was below the ordinary skill of an ordinary man exercising this particular art,[3] and causation can be proven, i.e. the sub-standard treatment led to harm. The duty of care, again, consists of three different aspects: the risk of harm is foreseeable, a sufficient proximity exists between healthcare professional and patient, and it is fair, just and reasonable to impose the duty of care.

If, in an EHR, patients are responsible for maintaining the record, this liability could shift. If they transfer data from the GP's/clinician's record into the EHR, the question is whether responsibility for accuracy rests with the GP/clinician or with the patient. If, due to a mistake in the EHR, the patient receives a wrong treatment, can the doctor be held liable? For the treatment to be negligent, the duty of care a doctor has towards a patient is not in doubt. This duty must have been breached. In this case, we need to take only the actual treatment into consideration and not the record entry. The reason for this is that if we were to expect doctors to monitor the patient's record entering,

---

[2] The much discussed *Bolam* test, derived from *Bolam v Friern Hospital Management Committee* [1957] 2 All ER 118, [1957] 1 WLR 582

[3] *Caparo Industries plc v Dickman* [1990] 2 AC 605; [1990] All ER 568 (HL)

the procedure would be severely lacking in efficiency. Thus, the existence of a breach of this duty is unquestionable – the patient received the wrong treatment. Finally, we will need to consider causation, i.e. which act has caused the ill effect on the patient's health.

At this point, the explanation turns problematic: prima facie, the wrong treatment, without doubt, led to the patient being harmed. The question, however, is, when and where we need to start looking for causation. Do we start at the beginning of the treatment? Or shouldn't we rather look further back to the hospital doctor consulting the records? And won't that lead us even further back to the point where the mistake in the entry occurred? If we follow that line of reasoning, then this leads to the rather astonishing conclusion that the patient herself must be held liable for the harm she suffered. On the other hand, however, should we consider it part of the healthcare professional's duty to check the accuracy of the record? Would it not be negligent to proceed on the basis of the record alone? If we were to expect this, then, as mentioned above, the system would lose much of its efficiency. It would, however, depend on the setup of the record. If the record is monitored and checked immediately after the patient has entered the details, then the healthcare professionals could certainly be held liable for not noticing the mistake. If, however, the record is only checked at certain intervals, or immediately before the information is required, then we could have a situation where, in an emergency situation, the record might not have been checked.

Similarly, in the shared model, these deliberations would need to take place. If both healthcare provider and patient are jointly responsible for maintaining the record, determining liability can prove a complex undertaking. Taking the above case, again, causation constitutes the problem. Only in this case, what if it cannot easily be determined whether the patient herself or the GP made the mistake in entering the incorrect information into the EHR. In the worst case scenario, a complex IT investigation would have to take place. It is perfectly possible for several people to have caused the harm and thus be jointly liable. It is very unlikely, however, that any record system would place all of the blame on the patient, but chances are that the nature of the liability as regards healthcare professionals will shift if the error in record keeping is indeed to be found to rest with the patient.

For the trustee model, it is obvious that the fiduciary cannot be held liable as he only keeps the records, but does not maintain them or add to them. Like the shared record, liability will have to be determined through deliberating who holds overall responsibility for the entry in question.

The last model is the electronic version of the current paper record in an improved way. When attending hospital as an outpatient without having been transferred by their GP, patients are currently given a print-out of their diagnosis and any prescription to hand over to their GP. Patients themselves would have to be responsible for any decline in their health due to failure to hand the print-out over. With the new EHR, this patient involvement will no longer be required, hence, patients won't be responsible for inaccuracies in the record.

2.1.3. The outcome

Several factors will need to be taken into consideration when recommending one or the other of the four models. First, logistics will need to be examined to determine which of the four types of EHR setup is the most technically feasible. Second, the

time management issue will have to be considered, i.e. if patients have a stronger involvement in creation of the record, is it feasible to monitor the respective input. And, finally, it will have to be decided whether it is in the patients' interest to have greater influence over the record creation or whether the task should remain in the hand of healthcare professionals.

3. Access to records in healthcare

The main legal problem arising from the question of who will get access to the EHR relates to confidentiality issues. Many patients still consider the old model of care, characterised by the two-party doctor-patient relationship and confidentiality between them. Patients, however, are not just looked after anymore by just their family doctor, rather, there is an extended health care team now with fully linked datasets joining many different bodies. A fictitious example will serve to demonstrate the problem: the patient is collected by an ambulance from her home. She is then brought to A&E, where initial treatment takes place. Afterwards she is admitted to an intensive care unit in the hospital. Once her status is no longer critical, she is transferred to a normal ward. In the hospital, she may require physical therapy before being released. If these various bodies do not communicate, there could be a potential risk for the patient in terms of treatment. The EHR will facilitate the communication considerably, if, any healthcare professional will be able to access the data. At the same time, however, care will need to be taken that only authorised people have access to the patient's records. One potential difficulty will be discussed here, namely where will the line need to be drawn.

As regards the access problem, Social Services can serve as an example. While they *may* have an important role to play in some patients' care, once released from hospital, their involvement is not automatically given. So, should Social Services be included? A look at data protection law may provide an answer.

In the UK, the Data Protection Act was passed in 1998 to protect individual's personal data and safeguard them against unlawful processing. Personal data and sensitive personal data are defined as follows:

> *'S 1 (1) 'personal data' means 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, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual. S 2 In this Act 'sensitive personal data' means personal data consisting of information as to- (e) his physical or mental health or condition… '*

Such health data may only be processed, e.g. disclosed, if one condition each of Schedule 2 and 3 of the Act is fulfilled.[4] The two schedules contain conditions such as consent or the processing being in the vital interest of the data subject. For 'mere'

---

[4] http://www.opsi.gov.uk/ACTS/acts1998/80029--n.htm#sch2

http://www.opsi.gov.uk/ACTS/acts1998/80029--o.htm#sch3

personal data, only one condition needs to be fulfilled, but for sensitive medical data, more stringent requirements are set and two conditions need to be fulfilled.

Usually, consent to data processing is considered the be all and end all, providing the person processing the data with the legal approval. However, frequently it is overlooked that consent is only one factor to legitimise data processing. The two schedules in the Data Protection Act offer a whole host of other possible justifications for legitimate data processing. One of those in Schedule 2 is that processing has to occur in the vital interests of the data subject. Schedule 3 contains that processing, i.e. disclosure of the record, 'is permitted 'for medical purposes, which includes preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.

Clearly, this is unproblematic for all those mentioned above in the fictitious example, as they are involved in the patient's care. But what about, for example, Social Services who are only involved in a percentage of cases?

Schedule 3 8 (2) expressly includes 'the provision of care and treatment' in the definition for 'medical purposes'. What needs to be decided is whether 'care and treatment' will need to be read together as one item or whether they will need to be interpreted as 'providing care *and* providing treatment'. If we agree on the latter, then providing Social Services with access is unproblematic. Or should we err on the side of caution and prefer the narrow interpretation? If we apply linguistics and consider the structure of the sentence, then the narrow interpretation would be more accurate – each individual purpose is separated from the others by commas and two conjunctions. Since in a properly structured syntax the conjunction 'and' is only used to link the last two parts of the sentence, the conclusion can be drawn that 'care and treatment' should be read together. If we accept this, then there is a strong case for not providing Social Services with access to the data.

Schedule 2 4 introduces a broader notion by permitting data processing when it is necessary in order to protect the vital interests of the data subject. If, however, the situation does not call for Social Services' involvement, it could be argued that the vital interests of the patient are not affected.

In both cases, whether we consider Schedule 2 4 or Schedule 3 8, the outcome depends on the point of view. If we consider the individual patient, then the above argumentation would apply. If, however, we were to consider the broader picture, i.e. look at healthcare in general, then the situation would be different and either condition might apply. However, the Information Commissioner promotes a case-by-case approach in cases of doubt. This approach, however, is problematic for practical purposes, as it defies the purpose of the EHR – providing easy shared access.

4. Access to records for research

Another aspect, which will need to be taken into account is the fact that medical research is increasingly making use of patient records, particularly in large epidemiological studies such as biobanks.[5] While clinical trials are most often combining research with healthcare, biobanks only require the participant to donate a

[5] See for example for the UK Generation Scotland, http://www.generationscotland.com, and UK Biobank, http://www.ukbiobank.ac.uk/

blood sample and, usually, fill in a lifestyle questionnaire and answer questions about familial relationships. Hence, this paper will focus on biobank-type research. Again, as mentioned above, the main problem is confidentiality.

Participants in a biobank give their consent for their medical records to be accessed by the biobank staff. Two problems, however, arise: In the first fictional case, the researcher, also a healthcare professional with access to all records, accessed the participants' parents' EHR? In the second fictional case, the researcher is not involved in healthcare. Should she be granted access to all health records to access the participants' parents' data?

In the UK, a culture of caution has arisen concerning the Data Protection Act with regard to research. This has taken on alarming dimensions, with some commentators arguing that the law now hinders research.[6] If we were to follow the letter of the law, however, than Schedule 3 of the Act needs to be taken into account, which states (2) In this paragraph "medical purposes" includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services. Hence, research is expressly included. In addition, s. 33 of the Act provides the so-called research exemption, which permits research on data previously collected, i.e. it permits data processing for a different purpose then the purpose for which the data were originally obtained. One obligation which neither Schedule 3 nor s. 33 obliterate, however, is that the data subjects have to be informed of the processing.

A recent report by the UK Academy of Medical Sciences (AMS) examined the problem and came to the conclusion that researchers should have access to personal data if they intend to anonymise said data for the actual research.[7] [7] As a result, it can be stated that in the current culture of caution, the use of participants' parents' EHR without their consent would not be acceptable. If, however, we were to follow the letter of the law and the AMS report, the result might be considerably different.

5. Conclusion

As the above demonstrates clearly, the application of information technology to healthcare and medical research is accompanied by considerable legal and ethical problems. Ideally, the multiple questions raised should be answered to a large extent before the EHR is converted from theory to practice. Hence, before adopting any of the four models or developing a different approach altogether, considerable more research will need to be performed into both technical feasibility of the model and its implications on both healthcare and research.

---

[6] Peto, J. et al, "Data protection, informed consent and research," (2004) *British Medical Journal,* Vol, 328, p. 1029

[7] Academy of Medical Sciences, Personal data for public good: using health information in medical research, January 2006