Medical research and data sharing – how open can we be?

Dr Renate Gertz
AHRC Centre
School of Law
University of Edinburgh
Scotland
Introduction
The uses of health data

• Primary uses:
  – For clinical care (relatively unproblematic)

• Secondary uses:
  – Research, epidemiology, public health surveillance, audit and service evaluation

• The overlap:
  – Clinical trials
The types of research

- Distinguish between two types of research:
  - Clinical trials (for clarity only those conducted as part of healthcare where HCPs = researchers)
  - Genetic research, ‘biobank’ type
- Different problems arise for both
- Main legal problems:
  - Data Protection (regulated by statute)
  - Liability (common law mechanism)
The current situation:
The CHI number

- 70s: Started life as the local Patient Master Index System in Tayside
- 80s and 90s: Slowly adopted by all Health Boards
- Name changed to Community Health Index
- → 8 separate CHI databases
- Each index contains all patients registered with a GP or who have been the subject of contact with Community & Preventative Care systems
- CHI database issues numbers from a unique range (= uniquely identifying)
• BUT: same person several CHI numbers
• → creation of another database – Search Index: allocates one CHI number as ‘current’ one, but does not hold full dataset, rather pointers to relevant records on the CHI databases
• → CHI = a linked series of regional databases
• Uses: Medical Record Linkage, Cancer registration, Remuneration of GPs, NHS24 may download CHI databases
The plan: Electronic Health Record

- Open data system throughout the health service
- Improve access to a current health record
- Prevent the so-called 'multiple-blood-test-syndrome' due to lack of communication between health care providers – sometimes even within the same hospital
- Facilitate research
The Legal Provisions
The law

• The Data Protection Act 1998
  – 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... Such health data may only be processed, i.e. disclosed, if one condition each of Schedule 2 and 3 of the Act is fulfilled
  – S 2: In this Act "sensitive personal data" means personal data consisting of information as to (e) his physical or mental health or condition,...
The Law continued

The first Data Protection Principle

“Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –

a) at least one of the conditions in Schedule 2 is met, and

b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.”
The Law continued

Schedule 2

1. The data subject has given their consent to the processing.

4. The processing is necessary in order to protect the vital interests of the data subject.

5. The processing is necessary … d) for the exercise of any other functions of a public nature exercised in the public interest.
Schedule 3

1. The data subject has given their explicit consent to the processing of the personal data.

3. The processing is necessary –
   a) in order to protect the vital interests of the data subject or another person, in a case where (i.) consent cannot be given by or on behalf of the data subject, or (ii.) the data controller cannot reasonably be expected to obtain the consent of the data subject, or
   b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

8. The processing is necessary for medical purposes (including the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services) and is undertaken by – a) a health professional (as defined in the Act), or b) a person who owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.
Secondary Uses of Data
Secondary use of data

• Research one of the most important secondary uses

• Problematic issue

• Controversial and contested: finding ways for secondary use that won’t compromise personal privacy

• Paper records and electronic records – different problems
Example Biobanks
Particularly problematic uses:

Example biobanks

- Biobank: combining and comparing biological tissue samples with genetic and historical patient information.
- Large epidemiological studies – biobanks are increasingly making use of patient records.
- Clinical trials often combine research with healthcare, Biobanks: only blood sample, lifestyle questionnaire and questions about familial relationships.
- Participants give consent for their medical records to be accessed by the biobank staff.
The Problems – an example

• The researcher, also a healthcare professional with access to all records, accessed the participants’ parents’ health records

• The researcher is not involved in healthcare. Should she be granted access to all health records to access the participants’ parents’ data?
Dissecting the problems

• Would this be wrong? Why?
  – Data protection/confidentiality issues
  – ‘sensitive personal 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
Dissecting the problems, continued

• Currently common practice: always obtain consent
  – Parents have not consented to their data being shared

• The problem: do we ‘fetishise’ consent? Aren’t there alternatives provided? And is consent practicable anyway in biobank research?
What does the law say – the ‘letter of the law approach’

• Schedule 3 of the Act needs to be taken into account:

• (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 than 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.
The AMS Report

- Report by the UK Academy of Medical Sciences (AMS) in 2006 examined the problem
- Conclusion: researchers should have access to personal data if they intend to anonymise said data for the actual research.
Conclusion 1

• 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.

• A decision is required = the wait for the first court case!
Introducing an Electronic Health Record
What may change?

• All healthcare professionals will have access to the EHR

• Researchers who are clinicians at the same time will have de facto access to everybody’s medical record

• Will new legislation be needed to regulate this access?
To opt out or not to opt out

• Policy in England: patients can opt out of EHR
• Tension between right to control what happens to information and society’s need for access
• Example cancer registers → Germany
• Reality: very little data processing in the UK done on statutory basis → basis of ‘implied consent’ → would fail if large numbers start to opt out
A different problem of openness and data sharing: Patient involvement in the EHR and the effect on clinical trials
Four models for an EHR

• The Personal EHR
  – patient as the chief manager and custodian of the record

• The Shared EHR
  – responsibility between patient and GP

• The Trustee Model
  – patients enter into contract with trustee, to keep and control the EHR

• The Interoperable EHR
  – Electronic equivalent to current system
Confidentiality issues

• **Personal EHR** – obviously less confidentiality problems, but: patients might approve access without appreciating wider privacy implications

• **Shared EHR** – depends where final responsibility lies – the more patient involvement, the less confidentiality problems

• **Trustee EHR** – patient decides what data will be transferred to trustee. But: trustee can break contract and process data → depend on the trustworthiness of the fiduciary

• **Interoperable EHR** – greatest risk of breaches of confidentiality as no patient involvement – stringent and enforceable access policy required
Liability issues

• Currently: error in the medical records leads to negative development in patient’s health, healthcare professionals responsible for error and subsequent treatment will be held liable

• larger patient involvement in creating and controlling the record may shift this liability

• First, liability will need to be explained, as UK system is fairly complex:
Liability in UK law

• Liability = non-contractual civil wrong.
• Main requirement: negligence
• Negligence has three requirements:
  – healthcare professional owes patient a duty of care
  – Breach of this duty has occurred (standard of treatment was below the ordinary skill of an ordinary man exercising this particular art)
  – Causation can be proven, (sub-standard treatment led to a legally-recognised harm)
• Duty of care has three requirements:
  – Risk of harm is foreseeable
  – Sufficient proximity between healthcare professional and patient
  – Fair, just and reasonable to impose the duty of care.
Liability continued

• If patients are responsible for maintaining the record and error leads to patient’s wrongful inclusion in clinical trial with negative outcome – shift of liability?

• Negligence? duty of care must exist – not in doubt.

• Breach of this duty – also unquestionable. (only the actual treatment to be considered – not record entry)
Liability continued

• Causation = problematic
  – wrong inclusion must have led to patient suffering a legally recognised harm.
  – prima facie: wrong inclusion led to patient being harmed.
  – But: When and where do we need to start looking for causation?
    • At the beginning of the treatment?
    • The hospital doctor consulting the records?
    • Won’t that lead further back to where the mistake in the entry occurred?
  – That line of reasoning → the rather astonishing conclusion that the patient herself must be held liable for the harm she suffered.
Liability continued

- Should clinician/researcher check record? Would it be negligent to proceed on basis of record alone? System would lose its efficiency.
- If record monitored immediately after details are entered – health care professionals liable for not spotting mistake
- If record monitored only in intervals or just before use, maybe no check in emergency
Conclusion 2

- Several factors to recommend one model over another
  - Logistics – which model is most technically feasible
  - Time management issue – if patients have a larger role – will monitoring be possible
  - Is it in the patients interest to have greater influence over the record
- Application of IT to healthcare accompanied by legal and ethical problems
- Questions should ideally be answered before EHR converts from theory to practice in Scotland