Medical Confidentiality and the Data Protection Regulation

This briefing note has been prepared for the Commission and for concerned MEPs. It sets out the background to medical confidentiality, including the history, the human-rights law, public expectations and the failures of previous regulatory regimes. It sets out why the compromise amendments on articles 81 and 83 of the Data Protection Regulation must be a red line, and why both the Commission and the Parliament must resist attempts by drug-industry lobbyists to undermine patient confidentiality. It is confidential as long as the compromise amendments are.

The writer is Professor of Security Engineering at Cambridge, a former adviser to the British and Icelandic Medical Associations, a former special adviser to the Health Committee of the UK parliament, and a member of the Nuffield Bioethics Council's working group on biodata.

Origins

Medical confidentiality goes back at least to Hippocrates, and has its roots in the requirements of clinical practice. If they cannot trust a doctor's discretion, patients will withhold information and this leads to real harm. Topical examples include

- The most comprehensive data were collected by the US Department of Health and Human Services prior to the HIPAA rulemaking under President Clinton. HHS estimated that privacy concerns led 586,000 Americans to delay seeking cancer treatment, and over 2 million to delay seeking mental health treatment. Meanwhile, over 1 million simply did not seek treatment for sexually transmitted infections[1].
- The Rand corporation found that over 150,000 soldiers who served in Iraq and Afghanistan failed to seek treatment for post-traumatic stress disorder; PTSD is believed to contribute to the suicide rate among military veterans being about double that of comparable civilians; a significant barrier is access to confidential treatment[2].
- The most authoritative literature review assessed a number of papers showing that many patients, particularly teenagers, gay men and prostitutes, regularly withheld information or simply failed to seek treatment because of confidentiality concerns related to sexually transmitted infections, sexual orientation and stigmatised behaviours. Anonymised HIV testing more then doubled the testing rate among gay men[3].

Medical confidentiality is not an abstract public good, but a critical factor in giving equal access to healthcare, particularly for at-risk, stigmatised and socially excluded citizens, but also for groups one might not think of as marginalised such as former service personnel.

---

[1] 'Standards for Privacy of Individually Identifiable Health Information', HHS 45 CFR parts 160–164, 65 Federal Register at 82461–82,510; see also 82,777–82,779

[2] 'Invisible Wounds of War', T Tanielian, LH Jaycox, Rand Corporation, 2008; p 128, 436

[3] 'Patient Perspectives of Medical Confidentiality – A Review of the Literature', P Sankar, S Mora, JF Merz, NL Jones, J Gen Intern Med. 2003 August; 18(8): pp 659–669

History of research ethics

The importance of medical confidentiality has long been recognised by the medical profession. However the profession does not always speak with one voice. Doctors with long-term care of individual patients, such as GPs and psychiatrists, tend to be very concerned about privacy; surgeons can be less so; while the minority of doctors who work in public health or research can be vocal advocates of getting access to other doctors' data.

Research has led to a number of serious abuses, which drove the development of research ethics.

- In the Tuskegee syphilis experiment, US doctors studied the progression of untreated syphilis in rural African-American men who were led to believe they were getting free healthcare. The experiment ran from 1932 to 1972, but even after effective antibiotic treatments became available in 1947, infected men were not treated.
- Dr Karl Brandt was Hitler's personal physician, and ran a euthanasia program from 1939. He also did human experiments on prisoners of war and the civilians of occupied countries without their consent, as did his colleague Dr Josef Mengele who experimented on twins at Birkenau from 1943–5; subjects were often killed and dissected afterwards. Brandt was hanged in 1948; Mengele escaped and died in Brazil.
- In the UK Alder Hey scandal, the press discovered that pathologists were routinely saving "interesting" body samples from patients living and dead, without any kind of consent. Parents discovered that body parts of their dead children had been kept without their knowledge. This did serious damage to public trust and the consequences have impaired research in pathology ever since. There was a similar scandal in Ireland.

The Nazi doctors' trial led to the Nuremberg code in 1948, under which the voluntary and informed consent of subjects is essential. The subject must have the freedom to choose, without deceit or duress, and must be able to exit from the experiment at any time. This led later to the Declaration of Helsinki on ethics in medical research in 1964, which was revised in 1975 after Tuskegee to incorporate the need for an independent institutional review board or ethics committee, and subsequently in 1983, 1989, 1996, 2000 and 2008. The Declaration is managed by the World Medical Association and is ethically binding on physicians. The Declaration upholds the right of patients to make informed decisions about participation in research, both initially and afterwards.

Until about the mid-1990s, the main ethical debates were related to drug trials: was it wrong to give placebos to HIV sufferers once effective antiretroviral drugs existed? And was it ethical to test drugs in less developed countries if their citizens or health services could not afford them? Since then, the growing issues have been informational: is it ethical to use whole populations as subjects in observational epidemiology and research, without giving them a right to opt out? And what are the ethical issues arising from low-cost sequencing of the human genome?

These issues came together in Iceland in the late 1990s: the government wanted to sell the nation's medical records for research in return for modern IT systems, but the Supreme Court objected and the enterprise failed. It did so on the basis of European law.

Legal background

The European Convention on Human Rights codified the right to privacy in 1948; states must respect privacy except where exceptions are necessary, proportionate and set out in law that is clear enough for their effects to be foreseeable. A later, more specific international provision was the Council of Europe Committee of Ministers' Recommendation No.R(97)5 on the Protection of Medical Data which elaborated standards for privacy in electronic health records, clarifying the exceptions and derogations reasonable for public health, health service management and research. This recommendation also started to engage data-protection concepts such as subject access rights with health IT. The EU's Article 29 Working Party on Data Protection has provided further guidance in the case of medical records, which specifically excludes the use of patient data for research without consent[4].

In 2010, the European Court of Human Rights decided the case I v Finland. Ms I was a nurse at a hospital in Helsinki who was HIV positive. The systems at the hospital enabled every clinician to see every patient's notes, and in consequence her colleagues discovered her HIV status, and hounded her out of her job. She sued for compensation, and the ECHR found that Finland had breached her right to privacy by failing to provide an environment in which she could keep her medical information confidential: "What is required in this connection is practical and effective protection to exclude any possibility of unauthorised access occurring in the first place."[5]

The national legal provisions among Member States vary rather widely, despite the Data Protection Directive. Denmark has a central research database of medical data, lightly de-identified by replacing the patient's name and address with a hash of their social security number (this is like the scheme adopted in Iceland but later found to be unsatisfactory by its Supreme Court). Germany has strict privacy law, which caused problems on reunification; the former East Germany had good cancer registries but the data had been collected by force; it took a lot of work to anonymise these to the standards required by West German law[6]. The UK had a free-for-all until 2000 when a central ethical review procedure was set up for non-consensual access to records; in 2013 the Government announced that records will by default be available for researchers under such a process but patients will have a right to opt out.

A complicating factor in the development of such policies has been anonymisation. Many researchers and policymakers had hoped that data could be scrubbed well enough to be not "personal" any more. But medical data cannot in general be made completely anonymous while still remaining useful for research. If successive healthcare episodes in an individual's life cannot be linked, then most interesting research cannot be done; yet if they are linked, then the publicly-known episodes or context in a patient's life can identify them, and the linking then exposes sensitive data. A summary can be found in the Royal Society's 2012 report on open science[7].

---

[4] Working Document on the processing of personal data relating to health in electronic health records (EHR), Article 29 Data Protection Working Party, 00323/07/EN WP 131

[5] I v Finland ECHR (Application no. 20511/03) 17/07/2008

[6] 'Clinical Record Systems on Oncology. Experiences and Developments on Cancer Registers in Eastern Germany' B Blobel, Personal Medical Information (1996) pp 39–56

[7] 'Science as an Open Enterprise', Royal Society, 21 June 2012

Public expectations

There have been many surveys of public attitudes to the use of medical data in research, and the findings are broadly stable across time and across countries. Most people are happy for their information to be used in research, so long as they are asked; if they are not asked but the data are simply taken, then most people are opposed. Some of the US surveys are cited in the HHS rulemaking (footnote 1, supra). UK surveys include Wells (1998)[8] and Robling (2003)[9].

The specific lobbying about articles 81 and 83

The lobby group "Science Europe" and its supporters such as the UK government and the Wellcome Trust (a UK research charity), have taken the lead in lobbying for the relaxation of articles 81 and 83 in the proposed data protection regulation. The Science Europe Position Statement however contains a number of misleading statements.

1. It wrongly states that "Pseudonymised data without access to decryption 'keys' make the possibility of re-identification of individuals very unlikely" and goes on to demand that "anonymisation must be explicitly stated to be outside the scope of the regulation". Yet the Royal Society report showed that anonymisation is not enough to preserve privacy.
2. It wrongly implies that re-identification risks can be controlled by decryption "keys" when the main risk of re-identification is from content and context.
3. The report seeks exemption from established data-protection law such as subject access and rectification as 'increasing the administrative burden'; yet they've been law for years.
4. The report claims "for some research projects it is not possible to seek consent at all from study participants". If patients cannot at least be granted an opt-out, then the research is currently unlawful. If the Regulation were to exempt medical research from data protection law, human-rights law would simply kick in in its place.

When resisting arguments put forward by big pharma lobbyists, the Commission must heed the risk that if drug industry researchers are deregulated, then eventually there will be a scandal which, like the Alder Hey incident, will do grave damage to public confidence in medical research – and in data protection. Control would pass from data protection law to human-rights law; privacy would prevail in the end but after an unpredictable legal process, at some cost in market fragmentation meanwhile, and with the risk that established systems would have to be re-engineered at great cost to comply with evolving law, as happened in Germany after unification. For all these reasons, the compromise amendments must be the Commission's red line.

Ross Anderson FRS FREng
Professor of Security Engineering
University of Cambridge, 22 May 2013

---

[8] 'Diabetic registers: a practice survey of patients' attitudes', M Wells, A Hassey, A Wilson, Health Informatics Journal Sep/Dec1998 vol. 4 no. 3-4 216-222

[9] 'Public attitudes towards the use of primary care patient record data in medical research without consent: a qualitative study, M Robling et al., J Med Ethics. 2004 Feb; 30(1): 104–109