The legalities and politics of health informatics

Jamie Grace

ABSTRACT

It may be some time before the coalition government can establish what the content of a Protection of Freedoms Bill would actually be; and how the content of such may materially differ from one another, as well as the effects these may have on the operation or longevity of the Human Rights Act 1998. The NHS 'engages' many aspects of the human right to respect for private and family life—not least through the emerging disciplines of 'e-health' and 'health informatics'. NHS data protection compliance standards, it is felt, will improve in the medium to long term as a data protection culture becomes embedded in newer ways of working with patient information, for example. Indeed, these standards must improve, lest NHS organisations fall afoul of the relatively new powers and sanctions afforded to the ICO. Health informatics programmes will be the driver for this systemic change—but paradoxically, the legal framework underpinning health informatics programmes, from a human rights perspective, could actually threaten the legitimacy of these selfsame health informatics programmes.

Databases operated by public authorities in the UK, including NHS organisations, have been praised and decried as many things, on a scale ranging from invaluable to Orwellian (Anderson et al, 2009; Anderson et al, 2007). Their lawfulness, rather than their morality or utility, is sometimes a thornier quality to measure. The suggestions from some quarters that the 'database state' comprises degrees of unlawfulness in the operations of different categories and purposes of public-sector e-governance have been firmly rebutted (Ministry of Justice, 2009).

Health informatics programmes are mainly legislatively enabled in the UK by the blandly-worded and broadly-described powers afforded the Secretary of State for Health in S.2 of the National Health Service Act 2006, as noted by the Ministry of Justice (Ministry of Justice, 2009).

This bland and ambiguous wording is in danger of being challenged through the courts via the Simms principle—which requires the clear and unambiguous wording of legislation to strip away our human rights. The NHS (and the Department of Health) must surely prefer a clearly-worded power to 'engage' peoples' information rights, as opposed to an ambiguous legislative wording that is constitutionally suspect—though sadly this is not currently the case for all NHS health informatics programmes.

Section 2(1) provides:

The Secretary of State may—

(a) provide such services as he considers appropriate for the purpose of discharging any duty imposed on him by this Act, and

(b) do anything else which is calculated to facilitate, or is conducive or incidental to, the discharge of such a duty.

Connecting for Health and Caldicott Guardianship

'Connecting for Health' is the banner under which the national programmes and policies for transforming healthcare in the UK through electronic governance are grouped; and the initiatives are strategically managed by the Department of Health.

Jamie Grace is Programme Leader for BA (Hons) Law, University of Derby, Derby

Email: J.Grace@derby.ac.uk

Submitted for peer review 12 August 2010; accepted for publication 26 January 2011

***

The NHS has given patients and service users a guarantee that their personal information will be well looked-after (NHS, 2007). Local responsibility for upholding this patient information standard falls to the holder of the 'Caldicott guardianship' for that particular local NHS organisation. Caldicott guardianships are co-ordinated nationally in an attempt to standardise the controls and protection of patient data (Connecting for Health, 2010a). The Department of Health is tasked with disseminating guidelines and good-practice with respect to these standards and others regarding patient confidentiality (Department of Health, 2003).

Care Records

The Summary Care Record (or the Emergency Care Summary across Scotland) is a nationally-accessible snapshot of the care a person has received from the NHS in the UK, that provides a limited medical record for any potential patient, and is designed to save vital time and avoid costly and potentially-fatal errors in pressured care and emergency contexts. Importantly, the SCR is 'opt-out' in implementation amongst cohorts of patients. Access is not particularly limited with regard to the number of NHS healthcare professionals who have the ability to use the SCR, but access is strictly controlled in terms of security and in the way the use of the SCR is audited on a user-by-user basis.

In a small study, less than 1% of people took the opportunity to opt out of the SCR. This creates a small but significant problem and some measurable loss of efficacy of the SCR programme. There are also ethical, if not legal issues around the choice of an opt-in system

It is of course S.2 of the National Health Service Act 2006 which the Ministry of Justice draws upon to assert the legality and lawfulness of the Summary Care record (Ministry of Justice, 2009).

In a small study conducted by this author, and using figures obtained through using the Freedom of Information Act 2000, it has been observed that less than 1% of people under the auspices of the Primary Care Trust in Dudley took the opportunity to opt-out of the SCR when such an opportunity was communicated to them. Scaled up across England and Wales, this still represents potentially hundreds of thousands of NHS patients who will initially or eventually opt out of the SCR programme. This creates a small but significant problem and some measurable loss of efficacy of the SCR pr ogramme. There are also ethical, if not legal issues, around the choice of an opt-in system for patient cohorts under the SCR programme.

The Ministry of Justice has noted that: 'A complex control framework limits access to the DCR to those involved in an individual's care (termed a 'legitimate relationship'). Access is by smartcard and an audit trail of all activity is maintained. Additional controls termed 'sealed envelopes' are being developed and these will enable a patient to restrict access to sensitive items within the record.' (Ministry of Justice, 2009).

This is just as well. The National Health Service is a vast composite organisation, and it

is essential for the protection of patient privacy, safety and confidentiality that access to an entire record of an individual's medical history and conditions be restricted to an appropriately local and specific division of any NHS organisation. The Detailed Care Record, as a patient information system, aims above all things to protect the integrity, quality and availability of patient data that will often prove vital in care contexts.

Again, the Ministry of Justice has sought to clarify the legality and lawfulness of this particular national database, but does not directly cite the provisions of S.2 of the NHS Act 2006 to support their rebuttal of legal concerns in this particular regard (Ministry of Justice, 2009).

Secondary uses service

The National Health Service in the UK has been challenged to transform the way that it uses patient information to conduct research which informs clinical practices (Connecting for Health, 2010b). This research is to be underpinned by April 2011 by the access a multitude of researchers will have to the 'pseudonymised' health data records of all NHS services users and patients. This notion of 'pseudonymisation', itself a technique of anonymising large data sets but retaining great statistical worth in them, allows NHS organisations to trade in this data for research purposes without falling afoul of the 'non-disclosure' provisions of the Data Protection Act 1998 and the common law of confidentiality (Ministry of Justice, 2009).

Again, the Ministry of Justice has sought to clarify the legality of this database (Ministry of Justice, 2009) by drawing on the wording of S.2 of the National Health Service Act 2006.

An important idea though is that while there may always be research and development of technical measures which help ensure the security of patient information in transformative healthcare settings (Huang et al, 2009), there may not always be a culture of protection and respect for human rights in healthcare; simply put, we can probably do anything securely with patient data; but what is ultimately to halt what we do with it?

Health and social care research

S.251 of the NHS Act 2006 allows for an application process, by which health researchers can receive permission from the Ethics and Confidentiality Committee of the National Information Governance Board of the NHS, through the delegated authority of the Health Secretary, to obtain entire, un-redacted, identifiable patient records for their use in research programmes. The Act clearly states that the common law of confidentiality is overridden in these circumstances.

Professor Dame Joan Higgins, formerly Chair of the Ethics and Confidentiality Committee (ECC) of the National Information Governance Board of the NHS, has noted that it is difficult to balance the need for the most effective health and social care research with the need to respect the sensitivities of patient confidentiality. However, there can be circumstances where society's need for effective research in the areas that impact upon public health outweighs notions of patient rights and confidentiality.

Higgins noted: 'In many ways, the greatest challenge for the ECC in the future is the same as the challenge which [Patient Information Advisory Group] faced when it began work in 2001. That is how to support high quality health care research, using patient information, whilst protecting the interests of patients and ensuring that their confidentiality is not breached. It is about making sure that an appropriate balance is achieved between these two goals. However, there have been some more recent changes which

create new pressures.

- It is essential that trust between patients and healthcare professionals, in the NHS, is maintained. Patients need to feel that whatever information they share with professionals will be held in confidence. If this trust is lost then the whole basis of care is undermined. Recent losses of sensitive data and inappropriate sharing of, and access to, health records may be starting to weaken this sense of trust.
- Increasingly, we are seeing requests from researchers to 'link' data for different data sets. This is essential for certain kinds of research but it also increases the risk of breaching confidentiality, not just where identifiable information is linked but also where anonymised information is linked but 'small numbers' (e.g. in specific geographical areas) may reveal patients' identities. There is no easy solution to this problem.
- Finally, there is the problem of third party information in patients' records. Ensuring that the confidentiality of third parties is not breached, as well as that of patients, is also a particular challenge.' (Higgins, 2009)

Data protection law in the UK

The effect of the 1998 Act

The Data Protection Act 1998 (DPA 1998) heralded the adoption in the UK of the EC Directive on Data Protection (Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data). There have been suggestions in the literature that the Directive could have been implemented with greater clarity (Robinson et al, 2009). In our common law jurisdiction in the UK issues of clarity will be resolved organically over time through the creation of precedents, as Lord Hope suggested (in Common Services Agency v Scottish Information Commissioner [2008] UKHL 47 at 47), when he wished that the Directive had been more directly incorporated into UK law.

Under the DPA 1998, individuals have the right of access to their own personal data, generally, and written permission is again, generally, required for the disclosure of personal data identifying an individual to another data controller. The word 'generally' is key, since these two core values of the DPA 1998 are subject to various exemptions.

Generally speaking, the operation of the DPA 1998 places duties on the controllers of personal data in the UK and affords certain rights to individuals in connection with their personal data. The working core of the DPA 1998 is the set of eight Data Protection Principles (DPP) which underpin the Act.

The most vital of the Principles is naturally the first (DPP 1)—which tells us that the processing of personal data must be done by data controllers in a way that is fair and lawful. This amounts to the notion that personal data must be treated as confidential, given that 'lawfulness' includes, in the UK at least, compliance and accordance with the common law (which evolves in the courts). For UK public authorities this entails affording all individuals due process rights and human rights in respect of processing their personal data, given our body of common law in the UK that addresses these administrative and constitutional legal issues, respectively.

The 'middle six' of the Data Protection Principles (DPP 2–7) afford rights to individuals—through placing duties on data controllers to respect the personal data of individuals in certain key ways: deleting it when necessary or when it is no longer needed, amending it to be accurate, and so on. Notable because of its inclusion in addressing practical issues is DPP 7, which requires that 'appropriate organisational and technical measures' be taken to safeguard data and the individual and

collective confidentiality of data subjects.

The Data Protection Act 1998, in including the eighth and final DPP, also seeks to regulate the manner in which the personal data of individuals is transferred between data controllers in the UK and data controllers and processors in different jurisdictions. The protection of data must be commensurate between the UK law and the law in any other jurisdiction to which data is transferred—not too much of an issue in EC territories, given the Directive (95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data); or for the USA, since the Information Commissioner here in the UK has determined that the American 'Safe Harbor' scheme is adequate data protection for transferral purposes.

From a wide perspective, the Information Commissioner has noted that our society in the UK evidences both positives and negatives when it comes to the protection of personal data, and hence personal, informational privacy.

Public authorities are not helped by some areas and practices concerning data protection and perceptions of the DPA 1998 being unclear and confused. The Information Commissioner has criticised the 'legal landscape' of personal informational privacy; while at the same time calling for UK public authorities to be more accepting of the need to share huge volumes of personal information in the name of better electronic governance; and to be bolder and more proactive in their approach (Thomas & Walport, 2008).

Public authorities, like NHS organisations, in breach of the DPA 1998 typically find themselves the recipients of an Enforcement Notice from the Information Commissioner; who is the relevant public body to conclude there has been a breach in some way. [replace?: the public body that decides if breaches have been made in this way]

KEY POINTS

- Electronic governance can and is transforming the way the NHS delivers healthcare
- The practicalities and ethics of e-health are separate, though still contentious, issues compared with the legalities of e-governance practices in healthcare.
- The legalities of e-governance practices in healthcare could be far more transparent, and the legislative empowerment of those practices could be far more unambiguous and purposeful. This would avoid the potentially costly situation of a systemic NHS e-governance project being declared unlawful in the scope or process of its operation.

Though there are criminal sanctions found within the DPA 1998—S.55 of the 1998 Act creates an offence of recklessly or maliciously losing or supplying data—prosecutions rarely result from data breaches.

The Information Commissioner has been granted new powers to fine organisations up to £500 000 for the most flagrant or severe breaches of the DPA 1998. Fines can be levied up to £500 000 under a Monetary Penalty Notice which can be issued under S.55A of the DPA 1998. It remains to be seen how organisations in the public and private spheres may adopt a different 'risk model' when it comes to caring about systematic compliance with the DPA 1998 now that there is the possibility of such large fines compared to the previous potential tariff of only £5 000.

Self-regulation and self-reporting, and the self-enforcement of data protection standards, is currently what the ICO expects organisations to undertake habitually in order to remain compliant with the DPA 1998. Certainly, the ICO has been encouraging businesses and public-sector organisations to think about the hidden costs through 'breach management' and 'disaster recovery', as well as public relations damage that sometimes occurs when a 'data breach' manifests itself as a leak or goes public. NHS organisations feature prominently in lists of concerning data protection breaches and information losses —showing only that they are vulnerable in the 'human error' sense of the design and operation of information technology.

Anderson et al (2007) Children's Databases—Safety and Privacy: A Report for the Information Commissioner, Foundation for Information Policy Research. http://tinyurl.com/6xau3gn (accessed 15 February 2011)

Anderson et al (2009) Database State, Rowntree Reform Trust. http://tinyurl.com/c44u8r (accessed 15 February 2011)

Aplin T (2007) Commercial confidences after the Human Rights Act. *EIPR* **29**(10): 411–419

Brazell L (2005) Confidence, privacy and human rights: English law in the twenty-first century. *EIPR* **27**(11): 405–411

Cabinet Office, Coalition Programme for Government (2010) http://tinyurl.com/2d984jh (accessed 15 February 2011)

Cartwright-Silk A, Carter-Hignett C (2009) A child's right to privacy: out of a parent's hands. *Ent LR* **20**(6): 212–217

Clarke RA (1988) Information Technology and Dataveillance. Communications of the ACM **31(**5): 498–512

Coates S (2009) Ethics could sink Tory plan for Google or Microsoft health records. *The Times,* 6 July

Connecting for Health (2010a) http://tinyurl.com/66bmk4j (accessed 15 February 2011)

Connecting for Health (2010b) http://tinyurl.com/676x5kc (accessed 15 February 2011)

Department of Culture, Media and Sport (2009) Final Digital Britain Report. http://tinyurl.com/5ta8j7a (accessed 15 February 2011)

Department of Health (2003) Confidentiality: NHS Code of Practice. http://tinyurl.com/5wh2rt (accessed 15 February 2011)

Foster S (2008) Balancing Sexual Privacy With the Public Right to Know: The Decision in Mosely v. MGN. 172 JPN 627

Grace J (2009) The data crisis in the UK. *J Law & Soc* **36**(2) (supp. Socio-Legal Newsletter: 6–7)

Grieve D, Laing E (2009) Reversing the Rise of the Surveillance State, Conservative Party. http://tinyurl.com/6ghs64b (accessed February 15 2011)

Gunasekara, G (2007) The final privacy frontier? Regulating trans-border data flows. *IJL & IT* **15**(3): 362–393

Higgins J (2009) Private correspondence with the author (J Grace) 14 September

Huang L et al (2009) Privacy preservation and information security protection for patients' portable electronic health records. *Computers in Biology and Medicine* **39:** 743–750

ICO (2008) Annual Report 2008/9. http://tinyurl.com/6dbxxc (accessed 15 Februry 2011)

ICO (2010) The Privacy Dividend. http://tinyurl.com/64jjxx8 (accessed 15 February 2011)

ICO (2007) Information Commissioner's formal response to the House of Commons Home Affairs Committee report 'A Surveillance Society?' http://tinyurl.com/5wz8e8 (accessed 15 February 2011)

Massey R (2010) Legislative Comment: Outsourcing—new standard contractual clauses for the transfer of personal data outside the EU. *CTLR* **16:**(4) 889

McLean A, Mackey C (2007) Is there a law of privacy in the UK? A consideration of recent legal developments. *EIPR* **29:**(9) 389–95

Ministry of Justice (2009) Government response to the Joseph Rowntree Reform Trust 'Database state' report. http://tinyurl.com/5sfn737 (accessed 15 February 2011)

NHS (2007) The Care Record Guarantee. http://tinyurl.com/4zudlw2 (accessed 15 February 2011)

Robinson (2009) Technical Report: Review of the European Data Protection Directive, Rand Europe. http://tinyurl.com/pc3088 (accessed 15 February 2011)

Thomas R, Walport, M (2008) Data Sharing Review Report, ICO. http://tinyurl.com/6s9vam (accessed 15 February 2011)

Wessels B (2007) Inside the Digital Revolution: Policing and Changing Communication with the Public, 1st Ed. Ashgate, Aldershot

***