scripted

Volume 11, Issue 1, April 2014

INFORMATION GOVERNANCE AS A FORCE FOR GOOD? LESSONS TO BE LEARNT FROM CARE.DATA

Dr. Mark Taylor[*]

DOI: 10.2966/scrip.110114.1

[*] Mark Taylor is a senior lecturer in the School of Law, University of Sheffield. He is also currently Chair of the Confidentiality Advisory Group for the Health Research Authority. Comments made in this paper are made in an entirely personal capacity and should not be taken to represent the views of the Confidentiality Advisory Group or the Health Research Authority.

Care.data has been in the news rather a lot recently.[1] What do the trials and tribulations of the programme, and the government's response, tell us about public and professional confidence in the ability of data protection law to effectively protect privacy in today's information age? What is more, how well does it illustrate, the capacity for information *governance*, as well as information technology, to shape society in the months and years ahead?

Care.Data

The Health and Social Care Act 2012 provided powers for the Health and Social Care Information Centre ('the HSC IC'), acting under direction from the Secretary of State for Health or NHS England,[2] to require the disclosure of confidential patient information by health professionals.[3] NHS England has directed the HSC IC to collect information from GP practices. The data collected from GP practices will be identifiable and will contain the patient's NHS number, date of birth, gender and postcode, together with a long list of 'read codes' that record clinical data of various types.[4] The 2012 Act provides a legal basis for such disclosure notwithstanding a lack of explicit patient consent. To the extent that information is provided in response to a request under the 2012 Act, the obligation of confidence that is owed by a health professional to a patient is expressly set aside.[5] In fact, the HSC IC is empowered to *require* the disclosure of confidential patient data from health professionals[6] and where it is necessary to disclose confidential patient information to meet a legal duty there is no breach of the common law duty of confidence by a health professional.[7]

Care.data has proven to be very controversial. A focus of initial concern for many was the fact that the 2012 Act provides no legal requirement to respect any patient

---

[1] A short selection of media articles would include: P Bradshaw "Care.data: trust is on the line" *Guardian Professional* 11 March 2014 available at http://www.theguardian.com/healthcare-network/2014/mar/11/caredata-nhs-trust-doctor-patient-leaflet; S Swinford "NHS legally barred from selling patient data for commercial use" *The Telegraph* 28 February 2014 available at http://www.telegraph.co.uk/health/10669295/NHS-legally-barred-from-selling-patient-data-for-commercial-use.html; N Triggle "NHS data-sharing project at risk, say MPs" *BBC News* 25th February 2014 available at http://www.bbc.co.uk/news/health-26347026

[2] Other bodies, and persons, are also entitled to request that the HSC IC establish information systems to collect information. In some circumstances the HSC IC must comply with such requests. The details are contained in s.255 and s.256 of the Health and Social Care Act 2012.

[3] See, in particular, s.254, s.256 and s.259 of the Health and Social Care Act 2012.

[4] A spreadsheet detailing the codes to be disclosed is available through the Information Centre website: http://www.hscic.gov.uk/media/12034/caredata-GP-data-specification/xls/caredata-gp-data-spec.xls

[5] Section 259(10) of the Health and Social Care Act 2012.

[6] Action by GPs to avoid this requirement was reportedly met, in at least one case, by a warning of termination of contract. See A Matthews-King "GP hit with contract notice over plan to opt all patients out of care.data" *Pulse Today* 4th February 2014 available at http://www.pulsetoday.co.uk/your-practice/practice-topics/it/gp-hit-with-contract-notice-over-plan-to-opt-all-patients-out-of-caredata/20005749.article#.UzrE3a1dUnY

[7] *Hunter* v *Mann* [1974] QB 767

objection to the disclosure of patient information to the HSC IC.[8] The argument was made, by a colleague, myself, and others,[9] that this was inconsistent with a number of existing legal principles and policy commitments.[10] Following the report by Dame Fiona Caldicott's Information Governance Review, where "to take account of the implications of the European Convention on Human Rights, the NHS Constitution and the views of people, the Review Panel concluded that reasonable objections from individuals must be considered",[11] there was a broadly welcomed policy commitment to respect patient objection.[12] While this commitment, and the more recent decision to place this on a statutory footing[13] represents good progress, the concerns expressed about care.data have always extended beyond simply respecting patient objection.

Perhaps chief amongst further concerns were those associated with transparency and oversight. In particular, concerns have been expressed about low levels of awareness. Despite the fact that the Data Protection Act 1998 places a responsibility upon data controllers to provide information, and leaflets were delivered to 26.5 million households in January, only 29% of adults polled for the BBC recalled receiving one.[14] The apparent low level of awareness amongst the public has been a particular concern for GPs who, as the data controllers for their patient records, are the ones under the 'fair processing' responsibility.[15] The 1998 Act does not sufficiently encourage co-ordinated activity between different parties where there are multiple data controllers engaged in parallel activities. Moreover, the responsibilities it establishes are, apparently, not sufficiently aligned with effective communication. This undermines the ability of the 1998 Act to protect privacy in other ways. For example, the value of respecting objection is obviously diluted if people are unaware of the disclosure to which they are entitled to object.

---

[8] R Todd, "Care.data IG reconsidered" *ehealth Insider* 27 March 2013 available at http://www.ehi.co.uk/news/EHI/8487/care.data-ig-reconsidered

[9] See comments attributed to Professor Douwe Korff, *ibid.*

[10] See, e.g. J Grace and MJ Taylor "Disclosure of Confidential Patient Information and the Duty to Consult: The role of the Health and Social Care Information Centre" (2013) 21(3) *Medical Law Review* 415-447

[11] "Information to share or not to share? Information Governance Review" (March 2013) at 79, available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf

[12] L Evenstad "Hunt pledges to respect patient data" *ehealth Insider* 26th April 2013 http://www.ehi.co.uk/news/ehi/8549/hunt-pledges-to-respect-patient-data

[13] For a discussion of this see, S Swinford "NHS legally barred from selling patient data for commercial use" *The Telegraph* 28th February 2014 available at http://www.telegraph.co.uk/health/10669295/NHS-legally-barred-from-selling-patient-data-for-commercial-use.html

[14] C Vallance "Adults "unaware of NHS data plans" *BBC News* 14 February 2014 available at http://www.bbc.co.uk/news/health-26187980

[15] A Matthews-King "GPs held responsible for patient complaints over NHS data-sharing project, says ICO" *Pulse* 10th January 2014 available at http://www.pulsetoday.co.uk/your-practice/practice-topics/it/gps-held-responsible-for-patient-complaints-over-nhs-data-sharing-project-says-ico/20005505.article#.UzrXF61dUnY

The problems with communication and transparency were heightened because people did not feel that sufficient assurances could be given regarding who would subsequently have access to their data, whether data would be in potentially re-identifiable form, and the purposes for which data would subsequently be used. The media contained reports of a number of disclosures by the forerunner to the HSC IC that undermined confidence in the ability of existing rules of information governance to retain public trust. Reports included disclosure to an actuarial society, reported under the headline "Hospital records of all NHS patients sold to insurers"[16] and a story about patient data being "uploaded to google servers" outside the UK.[17] This is a massively significant concern when the dataflow put at most acute risk by any loss of public trust is the disclosure of sensitive personal information by a patient to his or her doctor. It puts individual health care at risk.

In response to the public debate and widespread disquiet the care.data programme has now been 'paused' for (a further) six months. Dr Tim Kelsey, National Director for Patients and Information and the person responsible for the care.data programme, has said that one of the reasons for the delay is that it was not previously possible to give adequate "guarantees on how the data would be used".[18] The delay is intended to provide an opportunity to improve both the communication and the safeguards surrounding the programme. There is little doubt that the care.data programme provides an unprecedented opportunity to help people through the use of data: The opportunity to discover associations between co-morbidities, life events, drug combinations, and environmental factors is extremely significant. As well as the research it will enable, gathering the data will also allow enhanced national audits and service evaluations to check that individuals are receiving appropriate and effective treatment. This should pick up problems earlier and save lives. However, there is similar certainty that this must be done in a way that ensures, and is seen to ensure, that *public* benefits are achieved in ways that respect individual privacy.[19] Trust that data will only be used in ways that patients would recognise as appropriate must be preserved. The seeming inability of current law to offer adequate assurances regarding patient privacy led to a series of debates in Parliament (including two in Westminster Hall and a hearing by the Health Select Committee) and culminated in the government amending the Care Bill passing through Parliament.

Government Response

---

[16] L Donnelly, "Hospital Records of all NHS patients sold to insurers" *The Telegraph*, 23 February 2014 available at http://www.telegraph.co.uk/health/healthnews/10656893/Hospital-records-of-all-NHS-patients-sold-to-insurers.html

[17] R Ramesh, "NHS England Patient Data 'uploaded to Google servers', Tory MP says" *The Guardian* 3 March 2014 available at http://www.theguardian.com/society/2014/mar/03/nhs-england-patient-data-google-servers

[18] L Evenstad, "Kelsey admits care.data use unclear" *ehealth insider* 19th March 2014 available at http://www.ehi.co.uk/news/EHI/9299/kelsey-admits-care.data-use-unclear

[19] The idea of privacy that I rely upon here is developed in MJ Taylor *Genetic Data and the Law* (CUP, 2012), Chapter 2.

The government introduced a number of amendments to the Care Bill to address concerns raised in relation to care.data. These included placing more rigorous controls around disclosures of data and extending the role of independent advice to the HSC IC. The safeguards do not apply exclusively to data collected by the HSC IC under the care.data programme,[20] but are intended to provide the guarantees that were otherwise found to be lacking. Among the changes proposed, the HSC IC will be placed under a general duty to "respect and promote the privacy of recipients of health services and of adult social care in England".[21] Additional restrictions on dissemination of information by the HSC IC include a requirement that information may only be disseminated if the HSC IC considers it to be for the purposes of "(a) the provision of health or adult social care, or (b) the promotion of health".[22] These changes are intended, at least in part, to address concerns regarding inappropriate commercialisation of health data. In particular, the fear that data would be sold to insurance companies.

In addition to extending the duties placed upon the HSC IC, the breadth of independent oversight has been extended. The remit of the Confidentiality Advisory Group (CAG) is extended. CAG is an independent expert advisory group, which already exists as a committee of the Health Research Authority, but the Care Bill puts it on a statutory footing. The CAG will now provide advice to the HSC IC in connection with the publication or other dissemination of data that, although it may have been through a process of pseudonymisation, is not anonymised.[23] The Bill also gives the Secretary of State regulation-making powers to set out the specific criteria that CAG will be required to take into account in giving advice.

The Under Secretary of State for Health, Dr Dan Poulter, announced in the House of Commons that it is intended that such Regulations will require CAG to consider, inter alia, both

> …that the purpose for which the data will be used should be in the public interest and for the provision of health and care services; [and] that any approved processing must respect and promote the privacy of patients and care service users.[24]

The CAG[25] already offers advice on protecting *both* the public interest in research access to confidential patient data *and* the public interest in a confidential health service. It currently offers advice on the application of the Health Service (Control of Patient Information) Regulations 2002. These Regulations cannot be used to support the use of identifiable patient data where practicable alternatives exist, such as the use

---

[20] Indeed, it is important to remember care.data is about data going *into* the Information Centre. The new safeguards relate to data that comes *out* of the in a particular form.
[21] Paragraph 45 of Commons Amendments to Care Bill [HL]
[22] Paragraph 45 of Commons Amendments to Care Bill [HL]
[23] Paragraph 49 of Commons Amendments to Care Bill [HL]
[24] Hansard 10 March 2014: Column 137.
[25] And predecessor bodies: The Ethics and Confidentiality Committee of the National Information Governance Board and the Patient Information Advisory Group.

of anonymised data or explicit patient consent. This applies a constant pressure to avoid the disclosure of identifiable information, without explicit patient consent, wherever practicable.

In those cases where there is no practicable alternative, there is still pressure to respect patient privacy and to meet *reasonable expectations* regarding use. The stated ambition of the CAG is to only advise disclosure in those circumstances where there is reason to think patients would agree it to be reasonable.[26] Recommendations for support typically include conditions requiring (a) engagement with representatives of patient or public groups to test the acceptability of accessing confidential patient data without explicit consent and (b) respecting *any* individual objection to disclosure. Collectively these expectations go beyond the more limited right to prevent processing contained in the Data Protection Act 1998, and, in cases where individuals are not directly consulted, encourages consideration of their interests as represented by broader patient and public engagement.

There are thus a number of ways in which, and reasons for which, the position taken by the CAG extends beyond any reconciliation between privacy and public interest currently achieved by data protection law. An insistence that efforts are made to ensure that, even when the public interest is invoked, data is only used when this is consistent with an individual's own reasonable expectations - a use that they might be said to have reason to accept as appropriate - is an important qualification on intrusion that data protection law does not yet broadly recognise. It respects the value of reasonable expectation inherent within the common law duty of confidentiality; a duty itself grounded in the public interest.

It is too early to say what position will be taken in relation to the extended remit but one must hope that the CAG continues to seek concrete ways to identify and only support uses which individuals have reason to accept as reasonable *especially* where there is an appeal to 'the public interest' in access. Public confidence in the use, but only the appropriate use, of patient data must be maintained.

To protect what and to serve whom?

In a society that is not only information rich but also increasingly information dependent, the structure and governance of information flows is central to the growth and governance of society itself. As we seek to anticipate, plan, and construct a digital infrastructure capable of delivering the right information, to the right people, at the right time, there are multiple profound questions about whose interests the data must serve in the long term. Who are the right people, what is the right information, and what would be the right uses of data? The debate around care.data has at times reflected the tendency, seen in (data protection) law, to consider the public interest as

---

[26] HRA CAG 'Principles of Advice' (HRA 2012) at 4 available at http://www.hra.nhs.uk/documents/2013/09/v-2_principles_of_advice_-_april_2013.pdf .

something opposed to the protection of an individual's fundamental rights and freedoms. There will undoubtedly be times when one must give way to the other but to present them as necessarily opposed can place too great an emphasis upon their differences. It invites judgment that when the public interest justifies it, then individual privacy may be sacrificed. This is an unhelpful way of framing important questions. It does not sufficiently recognise the public interest in privacy protection or the ways that using data for public interest purposes, where it is *consistent* with people's expectations and preferences, can respect privacy. In short, there are many ways and times that we can seek to improve protection of *both* privacy and the public interest in access simultaneously without having to sacrifice one for the sake of the other.

It is not only in relation to health data that the ability of the law to protect *both* privacy and the public interest has come under challenge recently. The care.data debate has been carried out in an atmosphere tainted by the Snowden revelations. The basic principle of transparency is subject to limitations when necessary to protect various 'public interests' but the European Commission have expressed concern that, in the case of US surveillance of EU citizens, the US have been adopting an unjustifiably broad interpretation of necessity.[27] The broad point here is that the invocation of public interest arguments can be understood to trump fundamental rights and freedoms and this can be done without it being sufficiently clear how 'the public interest' is being defined or how the privilege afforded it in particular circumstances is justified to the persons affected. Individuals, uncertain of the model of public interest being applied, cannot be sure the extent to which their own interests are being respected. To put it simply, without a clearer determination of what is meant by 'the public interest', there is understandable concern that any given individual's interests might be sacrificed 'for the greater good' with that 'good' being defined and enjoyed by others.

To bring the example back to health research, there are some specific and current problems with the notion of public interest, and its relationship with privacy, being under explained in law that extend beyond care.data. The European Commission has proposed a General Data Protection Regulation to replace the Data Protection Directive that currently establishes the data protection framework across the EU. The text of the Regulation passed by the European Parliament allows individual member states of the EU to provide exceptions to the requirement to seek individual patient consent before health data are used for research purposes with regard to research that "serves a high public interest".[28] If the law relating to health research is to be better harmonised through the passing of a Regulation (rather than the existing Directive 95/46/EC), then we need a much better developed understanding of 'the public

[27] Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the perspective of EU citizens and companies established in the EU (Brussels 27.11.2013 COM(2013) 847

[28] Article 81(2)

interest' than is currently offered by law. What is more, we need an understanding that will not leave patients uncertain as to when or why an individual's expectations and preferences regarding access to and use of his or her sensitive data will be overridden – a national leaflet drop cannot reconcile privacy and public interest in the way that is needed. Simply 'providing' people with information is not enough to ensure that reasonable expectations are respected.

We need to do this better. There are classic examples of how gathering and linking data has enabled important insights - e.g. smoking and lung cancer - and of times when an inability to make the links quickly enough has had tragic consequences - e.g. thalidomide. The idea of the public interest needs to be developed to make clear that the reasons for such use must be accessible to members of the public. Those reasons also need to be subject to reasonable challenge by the public if they do not consider their interests to have been taken conscientiously into account by a specific activity. The public interest should only be called upon to defend interferences that individual members of the public can be given reason to accept. If people have confidence that data will *only* be used in ways that they have reason to accept, even when any legal requirement for individual informed consent may be formally overridden by the demands of 'the public interest', then the social legitimacy of the systems will be promoted. Particularly when dealing with sensitive data, such as the health data that the care.data programme is intended to handle, this is important. Not only because the programme itself depends upon people volunteering data to health professionals but because their health care depends upon it. New data architecture can dramatically enhance and improve existing uses of data. If such uses extend beyond those that individuals' might currently expect, or accept, then there are risks posed to existing uses of data. The six month pause that has been announced on the roll out of the care.data programme is an important time to work on these issues. However, we cannot expect to have all of the answers in six months time. The commitment must be an ongoing one to continue to consult with people, to continue to work to optimally protect *both* privacy and the public interest in the uses of health data. We need to use data but we need to use it in ways that people have reason to accept. Use 'in the public interest' must respect individual privacy. The current law of data protection, with its opposed concepts of 'privacy' and 'public interest', does not do enough to recognise the dependencies or promote the synergies between these concepts.