

Why might National NHS Database proposals be unlawful?

Dr Paul Thornton MPH, MRCGP
January 2006

5

Introduction

10 The Government's proposals for computerised National NHS Patient Records carry grave & imminent risks for both civil liberties and public health. They need urgent independent judicial review. The legal justifications used to substantiate their proposals are untested in the courts and require independent judicial clarification.

15 A complex draft consultation paper¹ circulated recently by the Department of Health confirms that highly sensitive data will be transferred from GP held databases to the nationally accessible database without the protection of recommended data "access controls". Ministerial reassurances to the public and parliament have been based on these access controls².

20 The consultation paper explicitly confirms that patient access controls, metaphorically dubbed "sealed envelopes", will be a primary means for achieving compliance with the common law requirement to allow patients to place restrictions on their confidential health information. But the same document goes on to confirm that the protection from "sealed envelopes"

- has not yet been designed and piloted.
- is not scheduled to be available until late 2007/early 2008 assuming it can be made to work.

25

And may never be able to hide information

- that forms part of an image e.g. a scanned letter
- that was first recorded on IT systems with record structures that are not compatible with sealing.
- after the patient's death.

30

The first data will be placed on the national database soon this year. It will be summary information taken from established General Practice systems.

35 Without the "sealed envelopes" the proposals cannot be reconciled with privacy legislation. But even if the proposals are implemented with the access controls as originally described there would still be clear grounds to question their lawfulness.

¹ "Sealed Envelopes" Briefing Paper Draft .NHS Connecting for Health
Document record ID Key NPFIT-FNT-TO-PRJMGT-0035.10 , Version 1.0 18/11/05
<http://www.ardenhoe.demon.co.uk/privacy/Sealed%20Envelopes%20briefing%20paper.pdf>

² <http://www.publications.parliament.uk/pa/cm200506/cmhansrd/cm050616/debtext/50616-37.htm>

40 Improved individual health care and effective public health protection would benefit from better
information flows between various individuals. But the most important information flow on
which all others depend is that from individual patient to individual clinician. These proposals
will inhibit that vital stage.

45 State control of all patient information is a dangerous civil liberties vulnerability. Privacy and
individual consent are the safeguards which prevent the practice of medicine becoming an arm
of state repression. The abuse of medical information contributes to the transformation of
democratic societies into totalitarian regimes. Privacy and consent prevent us drifting into
Stalinist psychiatry and the preventive medicine of the Third Reich.

50 Post war Germany and occupied Europe have had far more stringent control of patient
confidentiality than that in the UK. EU directed law bring us up to their standard and that law
should be properly applied.

55 The author has previously expressed ethical, philosophical and legal concerns with regard to the
National NHS Database proposals³. The purpose of this document to focus on areas of concern
in the law which should provide grounds for judicial review.

Background

60 It is intended that the National NHS Database will
include all the records made by all health workers in
respect of all patients in England. The database will
be accessible nationally to all those workers. The
Department of Health claim that they can record
65 patient information on such a database without
obtaining the consent, or even over riding the
expressed dissent, of patients.

70 Ministers have given separate assurances that patients
will be able to have their information excluded from
the database entirely if they so choose. However, this
choice is not protected in law as the law is currently
being interpreted, and there is no clarification of how
75 such an opt out will function. If the only alternative
being recognised is the use of pen and paper records,
this would be detrimental to the care of patients and
any consent could not be regarded as freely given.
Alternative computerised options such as the use of
local databases have been discounted by the
Department of Health.

80

The Department of Health have accepted & adopted advice that patients do not have a right to determine
where information is recorded about them. They claim that the recording of information on the National

Ethics Advisory Group Connecting for Health.

*“People should not be offered the choice to
opt out of recording their healthcare data on
National Care Records Service.”*

And

*“The EAG recommends that any decision not
to record new specific items of
data in the healthcare record rests with the
health care professional, who has
an ethical duty to record but who should, in
discussion with the patient, take
due account of the potential impact on
patient, healthcare professional, the
health service and society. Furthermore, it is
recommended that the incidence
of this is researched and the implications of
the findings considered by the
professional regulatory bodies.”*

³ <http://www.ardenhoe.demon.co.uk/NHS%20Database%20Privacy.pdf>

85 NHS database is distinct and separate from the dissemination of that information to others. Under their proposals, that distinction is false. Information recorded on the spine will be disseminated. The two processes are inextricably linked.

90 Even if the distinction was true, it provides little justification in respect of the Data Protection Act. The Data Protection Act restricts or allows the “processing” of data. “Processing” includes the simple recording or holding of data on any database.

95 If data is recorded on the national database by the GP there is a data transfer because the GP is currently an autonomous “Data Holder” and data on the national database would become out-with the GP’s control. Transfer of information from the existing GP database to the spine is self evidently a data transfer to the control of a different Data Holder.

95 The default arrangement will be that all recorded information on the NHS “Spine” will be shared with others.

100 The recent discussion document confirms that even if “sealed envelopes” are established to the maximum extent intended, health workers will be able to over-ride the patients wishes and access sealed information. According to the document, to be lawful, health workers will have to be able to justify this in terms of either

- Public interest
- Access required by statute
- 105 • Access required by court order.

110 These justifications are familiar under established practice but the National Database scenario is fundamentally different. In established practice the clinician deciding whether patient confidentiality can or should be justifiably and lawfully overridden already has lawful knowledge of the information concerned. In this national database scenario, the clinician making the decision does not already have knowledge of the information concerned and, explicitly, is one of the third parties from whom the patient wanted to withhold the information.

115 So even if the access controls are established as originally promoted the national database will give rise to information release such as in the following scenarios.

1. By Health & Social Care Act provisions.
 - a. The introduction of these powers were heavily criticised by professional bodies and patient groups as excessive for the purposes intended.
- 120 2. In an “emergency” – defined by the person accessing the record.
 - a. It is entirely reasonable that some information recorded by doctors in respect of their patients would not be relevant or necessary in an emergency situation or if the patient had subsequently lost capacity. It is legitimate that some patients would wish to keep some information private such that they would not be divulged even “in an emergency” and even to other health care workers.
- 125 3. By third parties with “consent”, e.g. NHS occupational health departments –
 - a. where consent may not be freely given.
 - b. where access to the database records would inevitably result in the release of information which in the terms of the DPA is unnecessary, excessive or irrelevant. An edited report purposefully generated for the third party by an involved clinician better meets the requirements of the Data Protection Act in this regard.
- 130

4. By police and other judicial powers.

- 135 a. Under current practice, information release can only be through the GP who makes the record. Once the information is outwith the safe haven of the GP practice it could be released by anyone with access. Such individuals may be less robust, as an advocate of the patient, in defending protection of the data to the fullest extent allowed by the courts.
- 140 b. The DoH have been explicit that security services would not have direct “Hands on” access to the database. (Given the current interpretation of the law, an explicit change in the law may be required to protect even this assurance.) However the security services would not need to obtain “hands on” access to the database. Police powers to access data can be applied to anyone who has access to that data. These powers would not only be used to obtain information about individuals already identified. Once a national database is established, it would be inevitable that security services would seek to have that database searched to identify individuals who matched specific criteria. – height, weight,
- 145 race, blood group, date of injury, genetic/DNA information, sexuality, etc, etc

5. By the release of “anonimised” individual data.

- 150 a. In DoH v Source Informatics the DoH argued that consent was required for the dissemination of individual patient data even when the recipient was unable to identify the individuals concerned. The DoH lost that case and did not appeal when it became clear that had they been successful a large number of information flows within the NHS would have been confirmed as unlawful. This has given rise to the widely held notion that information can be freely shared provided that the patient’s obvious identifiers e.g. name, address and date of birth have been removed. On that basis substantial patient data is shared within the NHS and out with.

- 155 b. In the Source Informatics case, it was agreed by both parties that Source Informatics could not “deanonimise” the prescription information they received. **But the ability to deanonimise information is a function not only of the information supplied but of the information already available to the recipient.** For example, it would be quite easy to recognise the records of an individual from “anonimised” hospital records if the individuals age, sex and hospital admission dates were in the public domain. Similarly, researchers and hospital administrators may have access to identifying databases such that, by data matching, the records of individuals in “anonimised” databases can be identified.
- 160
- 165

6. Through unlawful access

- 170 a. The total number of data subjects and the capture of the complete population makes the proposed National NHS database an inevitable target for hackers. The risk is in proportion to the scale of the database.
- 175 b. The database will allow public internet access with the intention that individuals will be able to access their own records providing a further hackable route into the system.
- c. The biggest security risk in a database arises from illegitimate use by individuals with otherwise legitimate access to the database. That risk is directly proportional to the number of legitimate users.
- d. The contractual, professional and criminal sanctions which might be applied to perpetrators in respect of unlawful access are important as a deterrent but are wholly retrospective and cannot undo the unlawful information release once it has occurred. Many people with concerns about the abuse of confidentiality are unable to complain for fear of their information being divulged further.
- 180

7. Through a lack of subject autonomy outside the clinical setting via the subject access provisions
- a. The ability of individuals to obtain access to their records is fundamentally important and beneficial. It is proposed that patients will be able to do this over the internet. But many patients do not enjoy autonomy in their lives outside the medical setting context. Without the safeguard option of being able to keep records off the database entirely, or in part, individuals will be pressured by third parties such as employers, abusive partners, criminal elements – to divulge their own records.

Even if the access controls which had been proposed by Connecting for Health were to be implemented, it is reasonable that some people would still not want their data, in total or in part, on the national data base. The records of patients who “seal” information will be flagged so that all clinicians will know that they contain information that is sealed. Of itself, this will be stigmatising.

Common law.

With limited exceptions, the release of information obtained in the course of medical practice requires the consent of the patient.

This may be

- Explicit - the patient gives a clear indication of his or her wishes.
- Implied - the patient is made aware that information will be shared and is seen to raise no objection when provided with an opportunity.

It is essential for both that the consent is informed. Patients must be aware of the nature of the information flow and their options for restricting that information flow. Historically, communication between involved health care professionals has been undertaken on the basis of assumed implied consent. Established common practices for information sharing when consent could not be implied, because the patient was not informed, are unlawful even within the NHS.

The proposed “Care Records Guarantee” does not inform patients that Ministers have provided the option for information not to be recorded at all on the national database. (See below re DPA fair processing requirements)

The “opt out” which is being offered by the Department of Health relates solely to the limited ability of patients to restrict access to their national record.

The proposals intend the assumption of consent after the distribution of a National Care Records Guarantee leaflet. This is not sufficient to assume implied consent to the release of information onto the national database. The proposals do not meet the standard required by the previous Information Commissioner. *“It is clear, however, that for consent of any sort to be given, there must be some active communication between the parties. It would not be sufficient, for instance, to write to patients to advise them of a new use of their data and to assume that all who had not objected had consented to that new use.”*⁴ The burden incurred in securing explicit consent is little different from that required for *valid* implied consent.

⁴ <http://www.ico.gov.uk/documentUploads/Use%20and%20Disclosure%20of%20Health%20Data.pdf>

230

Consent must be freely given. Individuals should not be denied access to the proper standard of care if they decline consent to information flows. The proper standard of care requires good communication between involved professionals but a national data base is not essential to achieve this.

There is no provision in common law to routinely overrule the expressed dissent of the patient to the transfer of information. Exceptional circumstances must prevail in all such cases.

235

Human Rights Act⁵

The Section 8 privacy right is not an absolute right. It is a qualified right that allows a public authority to interfere where that interference is:

240

- In accordance with law;
- In the pursuit of a legitimate aim; and
- Necessary in a democratic society.

245

Given that a national database of this type would be unique to the UK, it is difficult to argue that it is *necessary* for the health records of all individuals to be recorded on a national database. It cannot be argued that there is no alternative method to fulfil the health care purposes. Other mechanisms exist for the sharing of relevant information between directly involved health professionals that do not involve leaving information on a national database. As a consequence, though some might regard the use of a database as desirable for the protection of health, the test of *necessity* under the HRA is not met. Some information on all of the people or all information on some of the people might be necessary, but the notion that it is necessary to record *all* the sensitive health data of *all* individuals on a single national database cannot be substantiated.

250

Data Protection Act Schedules 2 and 3

255

Similarly Schedules 2 and 3 of the Data Protection Act provide various conditions as alternatives to the consent of the data subject which if fulfilled can allow data processing. However, these sections also include a test of necessity⁶. For example, under Section 8 of Schedule 3 of the DPA, the processing of information “for medical purposes” can provide an alternative to the requirement for consent. The prime function of schedule 3 section 8 is to enable the medical care of the patient to continue if and when the patient does not have capacity. Schedule 3 Section 8 does not provide “carte blanche” for doctors and health authorities to ignore the wishes of patients.

⁵ '8.1. Everyone has the right to respect for his private and family life, his home and his correspondence.

8.2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.'

⁶ See para 11 & 12 of dca.gov.uk article referenced above.

260

If consent cannot be obtained, the circumstance must be sufficient to make the unconsented processing of information “necessary”. It follows from this that if a lawful alternative strategy exists to resolve the circumstances of concern to which the patient might consent, the alternative modus operandum renders any unconsented processing unnecessary. Schedule 3 Section 8 criteria could not be used to routinely bypass the dissent of a competent patient.

265

270

It follows that if a patient does not consent to the recording of their information on the national database but does consent to the recording of data on paper or on a database wholly under the control of the professional to whom the data was divulged, it would be entirely possible to fulfil any “necessary” data processing via that mechanism.

As now, direct communication can take place between individuals without the need to leave a copy of the information on the nationally accessible database.

275

A similar test of necessity applies across several other sections of both Schedules 2 and 3 of the Data Protection Act which might otherwise be used to circumvent the requirement for patient consent to the recording and/or dissemination of information.

280

The test of necessity is addressed in guidance from the previous Information Commissioner⁷ in 2002

“The Commissioner takes the view that when considering the issue of necessity, data controllers must consider objectively whether:

285

- *Such purposes can be achieved only by the processing of personal data; and*
- *The processing is proportionate to the aim pursued.*

This aspect of the First Principle is reinforced by the Third Data Protection Principle, which states that:

290

“Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed”.

The disclosure of personal data where this is not actually necessary would be likely to contravene this Principle.”

295

The test of necessity is also addressed in guidance from the Department of Constitutional Affairs⁸.

300

“In many of the conditions referred to it is required that the processing is 'necessary' for a particular function or purpose. In our view the word 'necessary' in this context encompasses s which are 'reasonably required or legally ancillary to' the accomplishment of the specified purposes, it is not limited to those matters which are 'absolutely essential' to the accomplishment of those purposes.”

The cases cited in this guidance in support of this broad interpretation of “necessary” describe particularly extreme examples that justify the unconsented release of information . The applicability of these cases to the circumstances of the national NHS database are wholly

⁷ <http://www.ico.gov.uk/documentUploads/Use%20and%20Disclosure%20of%20Health%20Data.pdf>

⁸ <http://www.dca.gov.uk/foi/sharing/toolkit/lawguide.htm#part5> Section 4 See para 11 & 12

305 doubtful. The DCA guidance goes on “*In determining whether processing is 'necessary' in any particular case the sensitivity of the data may be relevant.*” and “*Whether it is "necessary" will depend on the circumstances of the case, and the Courts will look at effects that the disclosure may have on third parties.*”

Other Data Protection Act Provisions

310

Section 10

The Information Commissioner’s Office has acknowledged that a patient may be able to prevent dissemination of their data via the National Database under Section 10 of the DPA. There is a complete lack of information with regard to the Department of Health’s intentions for meeting this obligation. This is crucially important and no information should be placed on the national database unless and until arrangements in this regard are clarified.

315

However, in using this section, the onus is on the patient to show that the processing is *unwarranted* and would cause *substantial* damage or distress. Though important, on its’ own this section could be an insufficient safeguard. It does not apply in respect of processing deemed *necessary* for compliance by any legal obligation to which the data controller is subject. Nor does section 10 apply if the processing is deemed to be *necessary* to protect the vital interests of the data subject. It would also be possible for the Secretary of State to bring in an order which could over-ride the Section 10 protection.

320

325

The Fair processing requirement

Data processing must be “fair” in the terms of the DPA. If there is no valid consent then processing may not be “fair”.

330

Fair processing requires the provision of guidance to patients explaining how their data will be handled. The National Care Records Guarantee is the draft document intended to fulfil that requirement. It fails to inform patients that they have been given the choice not to have their data recorded on the National Database.

335

Other statutory provisions

The NHS(VD) Regulations 1974

These place statutory restrictions on information flow in respect of information relating to the treatment and diagnosis of sexually transmitted diseases. These regulations apply to all clinical settings, not only to clinics established for genito-urinary medicine. Recording information about STI’s on the national database will breach that regulation even if access to that data could be limited to staff of the facility from which the data derives.

340

The Human Fertilization and Embryology Act

Section 33⁹ prohibits the disclosure of specified information relating to infertility treatment. Placing that information onto the National Database of itself constitutes a disclosure as it would pass outwith the control of the clinician creating the record. Inevitably access to that information by others will constitute a further disclosure.

345

⁹ http://www.opsi.gov.uk/acts/acts1990/Ukpga_19900037_en_2.htm#mdiv33

Conclusion

350 The purpose of this paper has been to articulate concerns about patient privacy and confidentiality that are held by many with regard to the proposed national NHS database. It is written in terms which I hope will facilitate consideration and debate of these issues within the legal profession.

355 Legal guidance has been made available that is designed to defend NHS institutions and individual clinicians from liability when operating under these National NHS Database proposals. But there is a startling lack of suitably qualified legal opinion that might derive from the perspective of a client seeking to maximize protection of his right to doctor-patient privacy.

360 The doctor (or lawyer) as a patient has no less need in this regard.

It is imperative that the circumstances of the National NHS Database are subjected to independent judicial review.

-----/-----

365

Dr Paul Thornton MPH, MRCP
General Practitioner
Pear Tree Surgery
28 Meadow Close
370 Kingsbury
B78 2NR

01827 872755

375

Email address paulthornton*beeb.net (Note asterix inserted for “spam” protection: please replace the * with an @)

380

The author is a General Practitioner with an interest in patient privacy and confidentiality law deriving particularly from a two year post based at Coventry Health Authority with the remit to develop HIV/AIDS care and prevention within General Practice and Primary Care. He was a member of the public health sub-group of the Caldicott Committee.

He is RCGP Nominee to the multidisciplinary, multinational EU working party investigating patient confidentiality and vulnerable patient groups www.eurosocap.org .

385

He is a computerisation enthusiast having been IT lead partner in two GP surgeries migrating from paper to computer records. He was the only GP member of the Information Technology Local Implementation Strategy group for the NHS in Coventry and Warwickshire prior to establishment of the National Project for IT.

390

This document is available on line

<http://www.ardenhoe.demon.co.uk/privacy/NHS%20database%20proposals%20unlawful.pdf>