

PATIENT PRIVACY; UK LAW TO EUROPEAN STANDARDS

OBLIGATIONS FOR THE NHS DATABASE

A report to the National Information Governance Board for
Health and Social Care

January 2009

Dr Paul Thornton MPH, FRCGP

Author Note

I have been a General Practitioner since 1989. I have been lead IT partner in taking two practices through to "paperless practice".

I have a particular interest in patient confidentiality and privacy arising from a two year post in 1995-6 based in the Public Health Department of Coventry Health Authority with the remit to develop HIV care and prevention within General Practice and Primary Care. I was recruited to the Public Health working party of the Caldicott Committee, a DoH review of patient information use in the UK.

A paper I prepared for the RCGP and BMA, when supported in part by the office of the Data Protection Registrar, was influential in amending joint guidance between the British Medical Association and the Association of British Insurers with regard to the content of reports provided by General Practitioners to insurance companies.

I was subsequently nominated by the RCGP to participate in the Eurosocap project, an EU sponsored multinational, multidisciplinary working group charged to produce European Standards on Confidentiality and Privacy in Healthcare. <http://www.eurosocap.org/>

I was the GP representative on the Warwickshire Wide NHS Local IT Implementation Strategy Group prior to the CfH developments.

Dr Paul Thornton MPH, FRCGP

Pear Tree Surgery
28 Meadow Close
Kingsbury
North Warwickshire
B78 2NR
Tel 01827 872755
Email paulthornton@doctors.org.uk

UK law to European standards; Obligations for the NHS database.

A report to the National Information Governance Board

Introduction

The National Information Governance Board (NIGB) for Health and Social Care is “*very concerned about DH proposals to allow health professionals or research professionals to use care records, without the informed consent of the patient*” and the board believes “*that this is a breach of good practice in confidentiality and consent and have questioned if there is a sound legal basis for it.*”

This clear assertion from the first annual report¹ of the NIGB is extremely welcome at this juncture. The Department of Health have been explicit in their intentions in this regard for some years.

NIGB concerns have been reiterated subsequently in interviews [\(ii,iii,iv\)](#).(See boxes)

This paper sets out to demonstrate that the standards now being demanded by the NIGB are already enshrined in UK law to an extent that the Government cannot renege as easily as it intends. Recent cases in the European Court of Human Rights support a collective opinion from Data Protection Commissioners from across Europe with regard to Electronic Health Records. These provide clear guidance that must inform decisions made in the UK courts. The NIGB will want to review the reliability of the lawful basis that has previously been claimed for the NHS database.

Lawfulness and legal opinion

The Department of Health intends to abandon the requirement to obtain patient consent before releasing identifiable records. They intend to do this as part of their proposals for an NHS constitution. New legislation is proposed to over ride the common law of confidentiality that

BBC Online

“When we give our health information to the health service we do it on a basis of trust and we assume our health information will only be used by the people who provide us with care,” he told BBC News.

“Once you have sent someone's records to The Sun you cannot take them back again, whatever the penalties.”

Daily Telegraph

“If people want to take part in research then that's fine, but to assume they somehow have a duty to take part I don't think is necessarily appropriate. I am not sure it is the best way to achieve the outcomes researchers want.”

Mr Cayton said: “The public do value medical research but they rightly want to be asked first. Consent and confidentiality are the building blocks of trust in the NHS, and it cannot be in anyone's interests including researchers to undermine that trust.”

Harry Cayton
NIGB Chair

has been evolved by UK judges over many years.

Such legislation would implement a suggestion made by Mr Richard Thomas, the Information Commissioner in conjunction with Dr Mark Walport of the Wellcome Trust. The recommendation was made in a report(v) commissioned by the Prime Minister subsequent to the HM Revenue & Customs

Daily Telegraph

"There seems to be a view in some parts of the Government that if you receive services from the health service then it is OK to have open season on your medical records."

"Neither patients nor doctors had been properly informed about plans to share that information with third parties"

"I think this is like the DNA database, the information may be taken for one purpose, but we don't know what controls would be placed on access to it. The fundamental point remains that if data about a patient is being used for the benefit of research, their permission needs to be sought first".

Dr Tony Calland, Chair BMA Ethics Committee and NIGB member.

data discs going missing but prior to the Prime Minister and public being informed that they had gone missing. The Prime Minister broadened the terms of reference for Thomas and Walport once news of the HMRC disc was made public.

On the face of it, such a recommendation is wholly incompatible with the Information Commissioner's warnings about sleep walking into a surveillance society. It is counterintuitive that the appropriate response to Government data mishandling is to erode the controls that individuals have over information about them.

This proposal for new legislation confirms that, currently, such unconsented information flows are unlawful.

This author raised concerns (vi) with regard to the lawfulness of the NHS database in January 2006. A number of questions were raised not just in respect of the common law requirement for confidentiality but also with regard to a series of requirements under the Data Protection Act and the Human Rights Act.

When the BMA brought these concerns to a "Summary Care Record working party", convened by the Health Minister at that time, Lord Warner, further legal advice was obtained by the DH from a QC. On the basis of that counsel's opinion, the public were reassured the proposals for the Summary Care Record (SCR) "are lawful". But that reassurance was only provided once the department had conceded a limited opt out for patients from the SCR proposals.

There was no equivalent reassurance in respect of the other CfH database components and the department has since declined to publish the opinion from the Queens Counsel.

Did that Counsel's Opinion address the requirements of the Data Protection Act, the EC Data Protection Directive and the Human Rights Act?

Was that Counsel's Opinion provided previously to members of the Patient Information Advisory Group? If so, which members?

Have all members of the NIGB been provided with sight of the opinion from Queen's Counsel previously obtained by the Department of Health?

Can the NIGB fulfil its responsibilities unless all members are fully conversant with the law in this area to the extent/limits that the Department of Health has been advised?

The lawfulness of more recent proposals?

Inadequate consent mechanisms & "Consent to view".

The recent University College report from Greenhalgh(vii) et al into the summary care record pilot sites demonstrated that the prior leaflet distribution and other promotional activities failed to inform patients of the intended records dissemination. It had been claimed that this prior information would be sufficient to secure the legal requirement for implied consent of patients for the release of their information. They did not meet the standard for consent set out by the previous Information Commissioner in 2002 in guidance (viii) that remains on the ICO website.

It has subsequently been announced that the transfer of data to the national spine summary care records is now intended to take place without patient consent. The new strategy places a requirement on some health workers to obtain "consent to view" from the patient. This does not fulfil the same obligation.

In addition, some 10 million patients (ix) have already had their data released onto a *detailed* care record database from which the clear barriers to widespread access are being dismantled with no new information being provided to patients, let alone valid consent. This system is being provided by a CfH contractor, TPP Systemone. Contrary to previous reassurances by Ministers about "role based access" and metaphorical "sealed envelope" software, the facility to prevent the patient withholding information from clinicians is being actively promoted as an advantageous^x selling point.

This transfer of information must have included many patients despite their explicit dissent provided in letters sent to their GP's using a model downloadable from www.thebigoptout.com . Similarly for other patients who indicated their wishes directly to the Department of Health using a proforma provided by

the Guardian (xi) newspaper. Those patient mandates are explicitly not limited to the Summary Care Record.

The Information Commissioner's most recent public guidance (xii) with regard to NHS Electronic care records predates this "consent to view" change and is vague and cautious, particularly with regard to detailed care records.

Is NIGB aware of any further guidance from the Information Commissioner's Office (ICO)?

Have "consent to view" and detailed care record proposals been fully scrutinised by the Information Commissioners Office?

Breach of international law / obligations

While the Government might bring about legislation to over ride common law consent requirements, there are robust grounds to believe that such information release would still be unlawful. It would still be in breach of obligations under UK laws that derive from European directives and law. The UK cannot unilaterally amend such obligations.

Professor Douwe Korff gave evidence to the House of Commons Health Select Committee (xiii) that the CfH proposals did not meet the requirements of the European Directive on Data Protection (xiv), implementation of which gave rise to the UK Data Protection Act.

Professor Korff drew the attention of the Select Committee to a working document "*The processing of personal data relating to health in electronic health records*" (xv) prepared by the Data Protection Commissioners from all the EU nations, grouped together as the "Article 29 working party". That document is an entirely expert review of the law as it applies to Electronic Health Records. The courts would be expected to take into account their consensus because their forum is established in law, by the EU Data Protection Directive, to facilitate the uniform application and interpretation of the law across the EU. At the time of the select committee report that working document was out to consultation.

Subsequent to the health select committee report, Mr Ben Bradshaw MP, Health Minister, wrote to my MP, Mr Jeremy Wright. In his letter (xvi), Mr Bradshaw claimed that "*We expect that the working document will be amended to better reflect the realities of team based modern healthcare and to allow for the impact of the UK domestic common law of confidentiality that runs alongside data protection requirements. The UK information commissioner is represented on the group that is drafting the*

document and his staff have confidence that the final document will not require any significant change to NHS record keeping or law.”

However Mr Bradshaw acknowledged that *“It is true that if this document were to remain unchanged and become accepted as the interpretation of the law that the European courts adopt in the future, questions might arise about NHS compliance”*.

In fact, Mr Bradshaw’s expectations have already been shown to be substantially misplaced.

1. The document has been adopted by the Article 29 working party without any amendment subsequent to the consultation.
2. The European Court of Human Rights has already set out interpretations of the law in two recent judgements that are wholly consistent with the Article 29 working party document.

Surely, the NIGB is the body that should now ask those important “questions that arise about NHS compliance¹”?

Article 29 Working Party

I am informed by the European Commission secretariat that no dissent was expressed by any of the Data Protection Commissioners, and particularly by the UK Information Commissioner, when the document was finally accepted at a meeting of the Article 29 Data Protection Working Party on the 18-19 February 2008. This is difficult to reconcile with the IC’s previous assurances that Connecting for Health proposals are lawful nor with his endorsement of the proposal for the unconsented release of identifiable data to researchers.

While the working party document is advisory, it is authoritative. The European Courts, and hence the UK courts, would need exceptional grounds not to take account of the working document in future cases.

The CfH proposals do not meet the standards in law identified by the Article 29 Working Party across a substantial proportion of their document. It is essential that the membership of the NIGB scrutinise that document in full. A listing of the discrepancies between NHS database proposals and the working party report would require replication of their entire document. It is a model of clarity and does not

¹ - Particularly so as Mr Bradshaw is now intending to erode that very same “UK domestic common law safe guard” upon which he previously relied.

require further reinterpretation. However, the following are a small number of examples from the many issues that arise for the NHS database proposals.

- That the demographic data provided by patients in securing health care in must be regarded as “sensitive” in the terms of the Data Protection Act, and therefore afforded a higher level of protection. The extent of access to the PDS has been justified on the grounds that the information is not sensitive.
- That consent would not be acceptable if it is given under a threat of non treatment or lower quality treatment.
- That opt out solutions will not meet the requirements for *explicit* consent.
- That while Article 8(3) of the European Data Protection Directive (and hence the UK Data Protection Act) can provide an alternative to patient consent where the processing is used for medical purposes,
 - The processing of the entirety of records on under Article 8(3) cannot be lawful.and
 - Article 8(3) does not allow for research purposes.

Are these provisions alone sufficient to demand scrutiny of the entire Article 29 Working Party document by NIGB members?

ECHR Judgments.

The UK courts must take account of established judgements from the European courts when interpreting the UK Human Rights Act and Data Protection Acts.

The relevant very recent ECHR judgements are as follows:

Firstly, **I v. Finland** (xvii) relates directly not just to detailed electronic medical records but to demographic data stored electronically and linked to records of attendance at a specific clinic.

In this case, a nurse had been attending a clinic for treatment of HIV infection. At the same time she was working in a different department of the same hospital. It became apparent that staff in her work

department had looked at her computerised clinic attendance record and she was denied subsequent employment. The court ruled that her right to privacy had been breached and she has been awarded compensation.

To use the NHS database, all staff must have a chip and pin identity card and all record accesses will show up on an audit trail. In addition, staff should only be able access the records of patients with whom their employing organisation has a "legitimate relationship".

All such safeguards were missing in this Finnish case.

Even so, large numbers of UK staff will be able, but not allowed, to access the records of large numbers of patients who are not under their direct care. The Patient Demographics Service and Summary care records are accessible to staff across England. Detailed Care Records will be accessible to huge numbers of staff who work elsewhere in the institutions and community organisations that are providing care to the patient, or even more widely throughout "health communities" that are likely to cover entire conurbations.

The security of the NHS database is therefore based on deterrent laws and retrospective employment sanctions on staff who access patient records inappropriately. Ministers have relied upon this when seeking to reassure the public and parliament about CfH proposals.

This ECHR judgment is clear that, though important, such legal mechanisms do not provide sufficient protection. Even if such safeguards had been in place in the Finnish case, the data controller would not have avoided liability. The court has confirmed that health care staff who are not involved in the care of a patient must be unable to access that patient's electronic medical record. The court concluded "*What is required in this connection is practical and effective protection to exclude any possibility of unauthorised access occurring in the first place.*"

Secondly, the **CASE OF S. AND MARPER v. THE UNITED KINGDOM** (xviii), is the recent case in which the ECHR rejected the English practice of retaining DNA profiles and samples from individuals who had not been charged or convicted of an offence. The court's analysis over turns the arguments of UK government lawyers in respect of privacy concepts and contains several references which would carry resonance to UK courts in respect of CfH proposals. These are reinforced as Health

Ministers have conceded that information stored on the Secondary Uses Database will be made available to the police.

The resonant issues include

An interference in the right to privacy

- that the concept of “private life” includes information of the type stored in medical records such as the physical and psychological integrity of a person, multiple aspects of the person's physical and social identity. Elements such as gender identification, name and sexual orientation and sexual life fall within the personal sphere protected by Article 8. Ethnic identity must be regarded as another such element. Article 8 protects in addition a right to personal development, and the right to establish and develop relationships with other human beings and the outside world. The concept of private life moreover includes elements relating to a person's right to their image.
- That the mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8. The subsequent use of the stored information has no bearing on that finding.
- That even if only a limited part of this information is actually extracted or used by the authorities and that no immediate detriment is caused in a particular case does not change this conclusion.
- That cellular samples contain much sensitive information about an individual, including information about his or her health.
- that an individual's concern about the possible future use of private information retained by the authorities is legitimate and relevant to a determination of the issue of whether there has been an interference. Indeed, bearing in mind the rapid pace of developments in the field of genetics and information technology, the Court cannot discount the possibility that in the future the private-life interests bound up with genetic information may be adversely affected in novel ways or in a manner which cannot be anticipated with precision today.

In accordance with the domestic law

- that the wording “in accordance with the law” requires the impugned measure both to have some basis in domestic law and to be compatible with the rule of law. The law must thus be

adequately accessible and foreseeable, that is, formulated with sufficient precision to enable the individual – if need be with appropriate advice – to regulate his conduct. For domestic law to meet these requirements, it must afford adequate legal protection against arbitrariness and accordingly indicate with sufficient clarity the scope of discretion conferred on the competent authorities and the manner of its exercise. The use of DNA data is regulated in England and Wales by Police and Criminal Evidence Act (PACE). Even this was deemed too vague in parts by the ECHR. There is no equivalent domestic law in respect of the establishment of the national NHS database, nor determining the detail of its use. The nearest approximation is simply a departmental statement of intent, the “Care Records Guarantee”. This has no basis in law. The department otherwise relies entirely on non specific claims of compatibility with the common law and the Data Protection Act. Even if such claims are correct they would not be sufficient.

Necessary in a democracy.;

- That other countries, (even within the UK!) have not adopted similar database arrangements.
- That the England & Wales and Northern Ireland appear to be the only jurisdictions within the Council of Europe to allow such widely accessible medical records.
- That UK practice was at variance with transnational guidance.
- That in the Court's view, the strong consensus existing among the Contracting States in this respect is of considerable importance and narrows the margin of appreciation left to the respondent State in the assessment of the permissible limits of the interference with private life in this sphere. The Court considers that any State claiming a pioneer role in the development of new technologies bears special responsibility for striking the right balance in this regard.
- That there exist only limited possibilities for an individual to have the data removed from the nationwide database or the materials destroyed.

CfH Research Capability Program

Connecting for Health's own “Research Capability Program” has very recently documented their understanding of the law in respect of research (xix). Even this CfH publication acknowledges a number of areas where there is a need for authoritative clarification. And this assumes that they are correct in the arguments where they believe there is already clarity. They make no mention of the

Article 29 Working Party document, obligations under the common law or requirements the Human Rights Act.

Conclusion

All of this adds up at least to a persisting reasonable doubt with regard to the lawfulness of Connecting for Health proposals.

Without a clear consensus in respect of legal obligations, any concept of various agencies functioning as “data controllers in common” is wholly flawed (xx). This is epitomised in the suggestion that Social Services and Health Services staff might have common access to the data generated in each setting and yet staff from each domain might function under different “care record guarantees”.

I look to the common law and these EC derived regulations to protect my own privacy and confidentiality as a patient. I would expect those patients who have confided in our practice to have the same opportunity. I would be loathe to participate in a data transfer to the CfH systems without the valid consent of the affected patients for whom we are currently the data controller. And even with consent, the CfH database proposals must otherwise be lawful.

In making these criticisms, I am mindful of the risk benefit analysis (xxi) commissioned by Connecting for Health. This demonstrated that, overall, the CfH system design would compromise care compared to other possible IT system designs because they will inhibit patients from sharing information with health professionals in the first place.

The Wellcome Trust and others might reflect that this would not only be detrimental to the provision of care but also to the validity of extracted data that is used for managerial or research purposes. There is no conflict of interest between good research and a requirement for patient consent or true anonymisation at source for most research purposes.

There is already a growing consensus that CfH should move away from the concept of a monolithic, enormous database. The law appears to demand such a redesign. It is essential that we move towards much smaller databases each under the control of specific clinical teams, truly fit for their purposes and proportionate. This is the modus operandum that had already successfully facilitated IT development across General Practice, within Laboratories and to some extent in Radiology prior to the CfH interventions. CfH methods to date have singularly failed to deliver further computerisation in most secondary care settings and clearly need radical revision.

Once, but only if, such departments are successfully computerised, they can be made to facilitate selective, secure, timely electronic communications one with another where such information transfer is genuinely required, necessary and *lawful*. Such a change in system design is more likely to facilitate successful implementation by providing better functionality for end users and therefore better data and message quality.

The way forward

Will the NIGB now ensure that the previously obtained QC's opinion is

- Published?
- Updated in the light of the subsequent developments set out here?
- Sufficiently comprehensive?
- Commissioned from the perspective of patients who wish to protect their privacy to the fullest extent, while still being able to access NHS health care?

and

- Subjected to further truly independent authoritative informed legal scrutiny?

The NIGB is clearly already addressing some of these issues. I hope this report will provide a constructive framework for the board to take forward its deliberations.

Dr Paul Thornton MPH, FRCGP

References

- ⁱ <http://www.connectingforhealth.nhs.uk/nigb/consultations/NIGB-Annual.pdf>
- ⁱⁱ <http://www.telegraph.co.uk/health/healthnews/3868076/Doctors-fight-plans-to-hand-medical-records-to-researchers-and-private-companies.html>
- ⁱⁱⁱ http://news.bbc.co.uk/1/hi/uk_politics/7749879.stm
- ^{iv} <http://www.dailymail.co.uk/health/article-1100385/Doctors-fury-government-plans-release-private-patient-data-research.html>
- ^v <http://www.justice.gov.uk/docs/data-sharing-review-report.pdf>
- ^{vi} <http://www.ardenhoe.demon.co.uk/privacy/NHS%20database%20proposals%20unlawful.pdf>
- ^{vii} <http://www.pcpoh.bham.ac.uk/publichealth/cfhep/002.shtml>
- ^{viii} http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/health_data_-_use_and_disclosure001.pdf
- ^{ix} <http://www.tpp-uk.com/latest-news-02dec08.htm>
- ^x <http://www.tpp-uk.com/emergency.htm>
- ^{xi} <http://www.guardian.co.uk/society/2006/nov/01/health.medicineandhealth2>
- ^{xii} http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/information_commissioners_view_of_nhs_electronic_care_records.pdf
- ^{xiii} <http://www.publications.parliament.uk/pa/cm200607/cmselect/cmhealth/422/7051002.htm>
- ^{xiv} http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf
- ^{xv} http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp131_en.pdf
- ^{xvi} http://www.ardenhoe.demon.co.uk/Bradshaw%20correspondance/BB_JW_29_08_07.pdf
- ^{xvii}
<http://cmiskp.echr.coe.int//tkp197/viewhbk.asp?action=open&table=F69A27FD8FB86142BF01C1166DEA398649&key=71800&sessionId=17185320&skin=hudoc-en&attachment=true>
- ^{xviii}
<http://cmiskp.echr.coe.int//tkp197/viewhbk.asp?action=open&table=F69A27FD8FB86142BF01C1166DEA398649&key=74847&sessionId=17185320&skin=hudoc-en&attachment=true>
- ^{xix} <http://www.connectingforhealth.nhs.uk/systemsandservices/research/docs/pd15.pdf>
- ^{xx} <http://www.ardenhoe.demon.co.uk/privacy/Controllers%20in%20common.pdf>
- ^{xxi} <http://www.nhsconfidentiality.org/wp-content/uploads/November%20-%20NHS%20Care%20Records%20Report.pdf>

