Under threat: patient confidentiality and NHS computing

Ross Anderson

Professor of Security Engineering
Cambridge University
www.ross-anderson.com

The UK government is building a national database of medical records, a project which many doctors oppose; in a Medix poll in November, over half of all GPs said they would not upload their patients' data without consent [1] [2]. The following week, a Joseph Rowntree Reform Trust poll revealed that 53% of patients oppose a central medical records database with no right to opt out.

A campaign, TheBigOptOut.org, was launched on the back of that poll to persuade people to write to their GPs opting out of having their data uploaded to the 'Spine' [3].

Controversy followed quickly when the Chief Medical Officer wrote to GPs telling them to report dissenters to the Secretary of State, a move that the BMA condemned as a breach of patient privacy [4]. Meanwhile, a Department of Health consultants' report criticised plans to protect sensitive data on the Spine using so-called 'sealed envelopes' [5]. So what effect might the NHS's National Program for IT have on patient confidentiality, in the particular context of substance abuse?

Early days

Some historical background may be useful. The NHS 'IM&T Strategy', launched in 1992, had the stated aim of 'a single electronic patient record, accessible to all in the NHS'. Once the implications had sunk in, the BMA objected, and there followed a high-profile debate in 1995-6 about the permissible extent of electronic information sharing.

I was commissioned by the BMA to write 'Security in Clincal Information Systems', a policy setting out how the safety and privacy of clinical information should be managed [6]. The nub of the debate was that the BMA (and the GMC at that time) insisted that the patient have control – that patient consent overrode all other considerations except in a small number of exceptional cases defined by existing law.

The BMA policy therefore set out how patient consent could be implemented in real systems; it turned out that this policy, and similar ones, could deal perfectly well with access controls in the immediate care environment. For example, a clinical information system developed by System C and used in a number of UK hospitals adopted a form of role-based access control to restrict record access to staff in a patient's ward or department [7].

The Department of Health, on the other hand, rejected patient consent and insisted that access should be based on 'need to know'. While 'consent' and 'need to know' may be kept more or less synchronised in the immediate care environment, their effects diverge greatly when it comes to secondary uses of clinical data.

A health service manager may decide that he 'needs to know' all diagnoses of alcoholism in the UK, to monitor care costs; does his 'need' prevail over the wishes of a patient who has told his GP in confidence of an alcohol dependancy?

In the days of paper records the problem did not arise, or was at least not so acute, as the department of Health normally only got its hands on the record after the patient was dead – and so could no longer sue for breach of confidence.

One interesting episode in 1996 was a demand that the police be given access to the database of the Prescription Pricing Authority. The Department of Health argued that they needed this in order to catch the occasional doctor who misprescribed heroin. The BMA objected but eventually decided that this was not an issue on which it was prudent to fight a major battle. The police got their data; but this did not stop Harold Shipman murdering dozens more people.

In any case, the conflict between consent and 'need to know' for access was referred to the Caldicott Committee, whose report discovered dozens of illegal information flows within the NHS [8]. For example, supposedly de-identified data relating to treatment for HIV was being re-identified, creating identifiable records on HIV/AIDS patients at the PHLS, without the patients' knowledge (let alone consent). The eventual response of the Government was the Health and Social Care Act 2001 which allowed the Secretary of State to declare any flow of health information to be legal, regardless of objections under the law of confidence or data protection.

A brave new world

Having decided in principle that administrative 'need-to-know' overrode patient consent, the Government found the path clear to launching the National Program for IT in 2002.

This envisaged all clinical records in England moving to a national system, with hospital and GP records being kept on centralised systems by contractors – 'Local Service Providers' (LSPs) in five regions, and some further national applications spanning the whole of England. Contracts were let and the program began in 2003.

Hospital systems are now being migrated en masse to approved new systems provided by the LSPs. This has led to many operational problems. For example, the fact that systems are 'hosted' – that is, the patient data from records to X-ray images are kept at an LSP hosting centre rather than at the hospital itself – makes operations critically dependent on the availability of the hosting service and of the communications to it.

One of the first hospitals to be 'rolled out' to the new system, the Nuffield Orthopaedic Centre NHS Trust in Oxford, lost a day's operations after a power failure at its hosting centre.

A future failure of the Internet could thus leave England's hospitals without access to medical records and radiology images, reducing them to operating under field-hospital conditions. There have also been many schedule and budget overruns, with one of the key LSP contractors leaving the program.

Problems with the new systems are so pervasive and severe that a group of 23 professors of computer science (of which I am a member) has called on the Health Select Committee to review NPfIT; and recently the responsible minister, Lord Warner, has resigned.

Mistaken identity

The case of Helen Wilkinson is instructive. A GP practice manager in High Wycombe, she found that she had been wrongly entered on central systems as a former patient of an alcohol abuse service. She objected and experienced great difficulty in getting the incorrect data changed or removed. In the end her MP called an adjournment debate in the House of Commons at which health minister Caroline Flint promised that the data had been removed, and that Mrs Wilkinson would continue to have access to NHS care in future. (The system in question, the NHS Secondary Uses Service or SUS, contains summaries of all secondary care episodes; it is used for research and for health service management tasks such as helping answer parliamentary questions.)

Some time later, when the data had actually been removed, it transpired that Mrs Wilkinson could not receive NHS care without further central records being created. She has since started a campaign (`www.TheBigOptOut.org`) to persuade patients to opt out of central data sharing [10].

How to opt out

The immediate target of `TheBigOptOut.org`'s campaign is a plan to upload a 'summary care record' of each patient in England to the NHS Care Records Service (CRS). This will be followed in due course by further data. Ministers' vision is that CRS will eventually include all NHS medical records, both hospital and GP, in England. Within a few years, these are all supposed to be hosted on systems run by the LSPs, and so they can be joined up to provide a single record supporting seamless care in accordance with the 1992 vision.

It is claimed that privacy concerns will be dealt with by means of role-based access controls, which will limit record access to clinicians who claim to have a care relationship with the patient. In practice this will mean checking a popup that says 'Please confirm that this patient has given you consent to view their shared record'; checking this box is bound to become a reflex action for clinical staff.

For sensitive data there will be 'sealed envelopes'. A recent presentation about these is blatant about their purpose: they are to 'build confidence', to 'dissuade patients from dissenting' and to 'enable sharing of PSIS messages' [11]. If a clinician outside the care group accesses sealed data, an alert will be sent to the group's privacy officer.

There is a further option for a record to be 'sealed and locked' whereupon clinicians outside the care group will not be aware of the record's existence [12] [13]. There is a suggestion that GUM clinics will generate data that is 'sealed and locked' by default.

However, other systems will have access to sealed and locked data; access will be granted where the law demands it, and data will be collected for use by the SUS. (SUS data will in time be 'anonymised' but as this means merely replacing your name and address with your postcode, date of birth and NHS number, the level of privacy provided is risible – as Caldicott pointed out.)

To facilitate such secondary record access, sealing will be accomplished by marking the data using HL7 codes created for the purpose, rather than by (for example) encrypting the data using a key kept on a patient card.

Sealing thus provides a rather strange form of privacy. If you seal your data, any other clinician can still get access to it; while if you seal it and lock it, some clinicians involved in your care will be denied access to it, but civil servants and researchers will have access as before.

Not only does this arrangement offer the appearance of privacy, rather than its reality, but so do the proposed mechanisms for 'opting out' of the upload of GP records to CRS: the approved protocol is that the GP will upload the relevant records for all patients, and then further upload a blank record in respect of each dissenter (whose actual records will also be retained centrally).

Thus all medical records in the UK will be available for DoH purposes. What about other arms of government, such as the police?

Drug users and young people beware

There will be some restrictions on police access – CRS records should count as 'excluded material' under the Police and Criminal Evidence Act (PACE), so police officers have to jump through slightly more hoops to get access to it. However, access can still be obtained if they can show that the material is likely to be relevant evidence, and this may be particularly relevant in the case of drug users.

There is a further data feed in prospect to the Home Office 'ONSET' system that tries to predict the likelihood that young people will offend. This system harvests, from a wide range of sources, data that are correlated with offending – which may include local social deprivation, school behaviour reports, a history of parental imprisonment, and relevant medical diagnoses such as ADHD.

This data collection has been criticised in a report to the Information Commissioner as likely to stigmatise children unjustly and quite possibly in breach of European human-rights law [14].

If this system survives the Information Commissioner's scrutiny and any subsequent third-party legal challenges, it is difficult to see how information on drug and alcohol use from CRS will not be used as an input. Child welfare system managers will want not just records on drug and alcohol abuse by youngsters, but also by their parents or carers.

In addition to SUS and CRS, a final concern is HealthSpace, a proposed system to enable patients to see and comment on their own medical records. There is a concern with such systems that vulnerable patients will be bullied into acquiring access (which could be as simple as requesting a password through the post) and then into disclosing information, for example to relatives or employers.

The challenges to patient privacy in the field of drug and alcohol rehabilitation are thus potentially severe. To sum up, let us consider how two particular third parties – a police officer, and a private detective – can get access to a patient's treatment history.

Police and commercial access to medical records

In the case of the police, there has been access since 1996 to the Prescription Pricing Authority, and so a prescription for Antabuse, disulfiram or methadone can be picked up (though only the third of these is thought to be of interest at present). Access can be obtained to medical records already, but it is difficult as a practical matter.

At present, the investigating officer would have to locate the suspect's GP, get a Crown Court judge to sign a PACE production order, and then take it round to the surgery. Even so, the desired data might not be present at the surgery, as the suspect might have been treated in hospital.

In future, each police force will have a single point of contact with the CRS administrators at each LSP, and – if the arrangements made already with phone companies are any guide – data access will be largely automated and very convenient.

Access for specific purposes, such as identifying children thought likely to offend, may be fully automatic and built into the infrastructure, rather than requiring a production order for each case.

The private detective's life will also be much easier. At present, the main way to gather personal health information is 'pretexting' – phoning up someone at a general practice of health authority who has access to the data and telling some plausible untruth over the phone, such as pretending to be a doctor involved in the target's emergency care. At present, this is also inconvenient as the detective has to figure out which GP or health authority to call.

However, once all health service staff have access to all patients' records, all it will take to access an unsealed record will be one corrupt NHS employee whose local privacy officer is less then fully vigilant. Even sealed envelopes will be open to a corrupt employee prepared to take a small risk of exposure. A worrying lesson comes from banking: until the mid-1980s, getting copies of a target's bank statements was hard, as it meant subverting a local bank employee; since then,

the banks have enabled any teller to look up any customer's account details, and the street price of bank statements has plummeted.

The consequences for the treatment of drug and alcohol abusers remain to be seen, but can probably be guessed. There is much evidence that people are more likely to seek help if confidential services are available; patients want not just to discuss their problems, but to retain some control.

Victims of child abuse are reluctant to contact the child protection services, and are more likely to contact Childline [15] [16]; and the law used to afford special protection to records of sexually transmitted diseases. It seems likely that, in the case of illegal drug abuse, patients will be loth to divulge offences if these are likely to come to the attention of the police.

Although I am aware of no research on confidentiality in the specific context of substance abuse, its erosion in England will surely fill that gap that in time. The NHS Care Records Service is a large-scale experiment, but one from which it will be difficult to go back; if trust is lost, it could take a generation to win back.

References

1. Medix UK plc survey (Q1066) of doctors' views about the National Programme for IT (NPfIT) – November 2006, at `http://www.medix.to/reports/106620061121.pdf`
2. J Carvel, "NHS plan for central patient database alarms doctors", The Guardian, Nov 21 2006, at `http://society.guardian.co.uk/e-public/story/0,,1953185,00.html`
3. D Leigh, Rob Evans, "Most patients reject NHS database in poll", The Guardian, Nov 30 2006, at `http://www.guardian.co.uk/uk_news/story/0,,1960170,00.html`
4. B Marsh, "Patients will be ignored over privacy of records", Sunday Telegraph Dec 4 2006, at `http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2006/12/03/nhs03.xml`
5. "Local sealed envelopes 'probably safer' ", E-Health Insider, Nov 28th 2006, at `http://www.ehiprimarycare.com/news/item.cfm?ID=2302`
6. R Anderson, *'Security in Clinical Information Systems'*, BMA, Jan 11th 1996, at `http://www.cl.cam.ac.uk/users/rja14/policy11/policy11.html`
7. I Denley, S Weston Smith, "Privacy in clinical information systems in secondary care", in BMJ, May 15 1999, vol 318 pp 1328–1331, at `http://www.bmj.com/cgi/content/short/318/7194/1328`
8. *'Report on the Review of Patient-Identifiable Information'*, The Caldicott Committee, Department of Health, December 1997, at `http://confidential.oxfordradcliffe.net/caldicott/report/`
9. NHS 23, at `http://nhs-it.info/`
10. See `www.TheBigOptOut.org`
11. M Oswald, "Sealed Envelopes Briefing Paper: 'Selective Alerting' Approach", NHS CfH document NPFIT-FNT-TO-IG-PRGMJT-0035, December 2006, at `http://www.connectingforhealth.nhs.uk/crdb/sealed_envelopes_briefing_v2_0.doc`

12. "Sealed Envelopes – Guiding Principles Document", NHS CfH document NPFIT-FNT-TO-REQ-DEL-0139, December 2006, at http://www.connectingforhealth.nhs.uk/crdb/sealed_envelopes_guiding_principlesv1-0.doc
13. "Sealed Envelopes", December 2006, at http://www.connectingforhealth.nhs.uk/crdb/sealed_envelopes.ppt
14. R Anderson, I Brown, R Clayton, T Dowty, D Korff, E Munro, *'Children's Databases – Safety and Privacy'*, Information Commissioner's Office, Nov 2006, at www.fipr.org
15. P Cawson, C Wattam, S Brooker, G Kelly, *'Child maltreatment in the United Kingdom: A study of the prevalence of child abuse and neglect'*, London, NSPCC, November 2000; at http://www.nspcc.org.uk/Inform/Research/Findings/ChildMaltreatmentInTheUK/Executivesummary_asp_ifega26228.html
16. A Weyman, C Davey (2004) *'The right to confidentiality: young people's access to sexual health services'*, Childright v 211 (2001) pp 6–7

This article: Drugs and Alcohol Today, v 6 no 4 (Dec 2006) pp 13–17