Patient confidentiality and central databases

Ross Anderson

Professor of Security Engineering
University of Cambridge Computer Laboratory
15 JJ Thomson Avenue, Cambridge CB3 0FD, England
www.ross-anderson.com

2008 may be the year when GPs find themselves in the firing line over confidentiality, as ever more patients try to opt out of 'the NHS database' and the Government tries ever more desperately to keep the project on track. But I believe this should not be seen as a problem, but an opportunity – a once-in-a-lifetime chance to make a decisive change. GPs, by acting as the patient's advocate, can not merely retain patients' trust and defend their professional autonomy, but also rescue health policy from a serious wrong turn.

Public concerns about the centralisation of health data have grown in recent years, especially since the press took up the issue in 2006. In November that year, a poll revealed that 53% of patients opposed a central medical records database with no right to opt out [1]. At the same time, a report for the Information Commissioner (of which I was an author) described government plans to share health information on children widely with other services, including social services, school teachers and the police. It concluded that the proposed measures were both unsafe and illegal [2]. In September 2007, the House of Commons Health Committee called for more information to be published on the proposed design, and for data placed in 'sealed envelopes' to be withheld from the Secondary Uses Service (SUS) – a suggestion that the Department rejected [3].

These concerns have since been brought into sharp focus by the government's loss of personal information on all the nation's children and their families last November. The Conservatives are now promising to end the National Programme for IT (NPfIT) and go back to keeping data on interoperable local systems where 'records should be owned by the patient, and stored locally, under the control and protection of his GP' [4].

The average GP's reaction will be 'and about time too!' Medix has conducted regular polls on NPfIT since 2003. Then, 67% of GPs said it was an important priority for the NHS; that's now sunk to 30%, while 70% of all doctors do not consider NPfIT to be a good use of NHS resources. Some of the strongest opposition is over confidentiality: 76% of GPs and 55% of other doctors think that NPfIT will damage confidentiality, while 59% of GPs and 49% of others say they will not, or are unlikely to, upload a patient's clinical details without specific consent [5].

GPs are in a hugely influential position for two reasons. First, they (still) control the lifetime patient record; and second, they are trusted by a large majority of patients because of their tradition of independence and of safeguarding information.

Of course, there is not just one 'NHS database'. The current opt-out campaign relates in the first instance to the Shared Care Record, which is being piloted in Bolton, Birmingham and Christchurch; this is being loaded with current medications and allergies initially, and is expected to contain much more later. A further concern is the move to hosted systems by many providers, in both primary and secondary care, which is making records available for central uses outside the effective control of the providers. GP records in particular, once hosted, are expected to be accessible across the local health (and social care) community.

Several national databases of identifiable health information already exist, ranging from the Prescription Pricing Authority's records of all prescriptions to SUS which contains identifiable data on finished consultant episodes in secondary care and from which the Health Committee believed patients should be entitled to opt out. Other national services have recently been built, such as the Picture Archiving and Communications System that centralises the storage of digital X-rays, and there are many plans for further data sharing in the public sector: the children's databases described above are to be followed by similar systems for the elderly and the mentally ill.

Without robust consent procedures and effective opt-outs, these systems will make it increasingly difficult for a patient to get any kind of NHS care without appearing on central databases. (I believe that, to stay within European human-rights law, the NHS will have to offer all patients the right to be treated under a pseudonym, as is currently the case with Armed Forces personnel.) But the immediate battle is not about the secondary uses of health information, so much as its primary uses. There are concerns about both privacy and safety.

Privacy and safety

Practical privacy issues with medical records are surveyed elswhere [6]. First, there's unlawful access to medical records, which at present largely involves 'pretexting' – phoning up someone at a general practice or hospital trust, pretending to be an NHS insider and telling some plausible tale. At present, this is inconvenient as the detective has to figure out which organisation to call; but it is still a frequent scam, and many cases have been detected. But once most NHS staff have access to all patients' records, it will be a whole lot easier – unless compensating controls are implemented. In September 2007, the Health Committee called for better operational security; the government replied that this already existed. (At least, that was their position just before the HMRC debacle.)

Second, there's lawful access. At present, a policeman who wants to see a suspect's records has to locate the GP, get a Crown Court judge to sign a PACE (Police and Criminal Evidence) production order, then take it round to the surgery. This is rare at present. But once records are stored in a few server farms, life will become a lot easier for the policeman too. This may be a real issue in drug and alcohol treatment; a judge could find it difficult to refuse the police access to all medical records in its region that contain admissions of drug use, as this is 'actual evidence' of crime; and ministers have just announced that that it will be a priority 'to ensure that families affected by substance misuse are identified earlier' [7]. The confidentiality of patients who admit to under-age sexual intercourse may raise similar issues.

Third, there's mission creep. There are many plans in Whitehall to make use of health data once they are conveniently available – education officials want to identify children with welfare issues, while the Home Office has a system, ONSET, which tries to predict which children will offend. Both plan to make extensive use of health data – as described in the report to the Information Commissioner [2].

Centralising clinical data on remote server farms can prevent some kinds of failure, but is likely to cause others. U.S. veterans who fled New Orleans after Hurricane Katrina found their medical records available wherever they went, as the Veterans' Health Administration has a centralised system. On the other hand, the VA has suffered repeated privacy compromises, including one incident in which they lost the social security numbers of all veterans, leading (as with Britain's HMRC case) to a nationwide alert.

And there are safety issues that have nothing to do with privacy: if records are only available on a remote central server, then a network outage or a power failure can be serious. The first UK hospital to go live with a remotely-hosted system, the Nuffield Orthopaedic Centre NHS Trust in

Oxford, lost a day's operations after a power failure at its hosting centre. Moving from an old way of working to a radically new one means trading well-understood risks for risks that are much less certain.

Finally, computer systems generally do the bidding of those who pay for them. A number of people involved with GP systems have remarked to me that development efforts are now being redirected into providing links with administrative systems rather than on improvements that would improve the quality of patient care. One may even ask whether it was wise, at the last GP contract negotiation, to accept the government's kind offer to pay for all the computers.

Britain needs to turn over a new leaf in healthcare IT. As in the Netherlands or Sweden, central government should restrict itself to setting standards for interoperability and maintaining an approved product list. GP Systems of Choice are a useful step in the right direction, but we need a real transfer of power away from the centre and to the people in the best position to tell suppliers what new systems should do. That means local rather than central purchasing – and by the practice or hospital, not the PCT. This is how things are moving overseas: no country is as centralised as the UK, and almost everywhere there is more progress. We should get back into the mainstream. In a globalised world, we will have to eventually. And the sooner we can consign Connecting for Health to history, the sooner we can get on with it.

Action

In Iceland, the government tried in the late 1990s to get everyone to sign up to a national medical database. GPs there were not impressed by the government's assurances of confidentiality, and left opt-out leaflets in their waiting rooms. Over 11% of the population opted out, and the authorities in Reykjavik had to abandon their plans to make the system universal.

The UK now also has a similar campaign, led by practice manager Helen Wilkinson, which has prepared opt-out leaflets that can be downloaded from its website, `www.TheBigOptOut.org`. I would like to ask all GPs to make these leaflets available in waiting rooms – or, alternatively, to write an optout leaflet of your own, as the Oakland Practice has [8]. Please provide a link on your web pages too – and provide a link to the Department of Health as well. Let patients hear both sides of the argument.

The British Medical Association line is that the Shared Care Record should be opt in, but the Government doesn't agree. The next best thing is to empower patients to opt out by showing that that you don't disapprove. The surgeries that have already tried this have found that from 6% to 19% of patients will actually fill out the form [8] [9]. Once several million more

join them, the political case for universal centralisation will collapse, as it did in Iceland. This will in turn empower both medics and IT professionals to work together and reshape medical informatics so that systems are both safe and responsive to clinical needs.

Ross Anderson

Competing interests: The author is an advisor to TheBigOptOut.org, a member of the group of computer science professors who called for a review of NPfIT (`www.nhs-it.info`), a former special adviser to the Health Committee's inquiry into the Electronic Patient Record [3], and a former advisor to both the Icelandic Medical Association and the British Medical Association.

References

[1] 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`

[2] R Anderson, I Brown, R Clayton, T Dowty, D Korff, E Munro, 'Children's Databases – Safety and Privacy', Information Commissioner's Office, November 2006, at `http://www.cl.cam.ac.uk/~rja14/Papers/kids.pdf`

[3] House of Commons Health Committee, "The Electronic Patient Record", September 2007, at `http://www.publications.parliament.uk/pa/cm200607/cmselect/cmhealth/422/42202.htm`

[4] David Cameron, "The NHS at 60", January 2 2008, at `http://www.conservatives.com/tile.do?def=news.story.page&obj_id=141441&speeches=1`

[5] Medix UK plc, 8th Survey on National Programme for IT (NPfIT) – November 2007

[6] R Anderson, "Under threat: patient confidentiality and NHS computing", Drugs and Alcohol Today, v 6 no 4 (Dec 2006) pp 13-17; at `http://www.cl.cam.ac.uk/~rja14/Papers/drugsandalcohol.pdf`

[7] E Milliband, B Hughes, "Think Family – improving the life chances of families at risk", Cabinet Office, `http://www.cabinetoffice.gov.uk/upload/assets/www.cabinetoffice.gov.uk/social_exclusion_`

task_force/think_families/think_family_life_chances_report.pdf

[8] The Oakland Practice, http://www.ymcentre.freeserve.co.uk/

[9] "A fifth of patients reject e-records", in Healthcare Republic, Jun 8 2007; at http://healthcarerepublic.com/news/GP/662815/fifth-patients-reject-e-records/

Citation for this article: British Journal of General Practice, Volume 58, Number 547, 1 February 2008 , pp. 75-76(2)