The Foundation for Information Policy Research

Consultation Response on

'An Information Revolution' – the latest NHS IT Strategy

The Foundation for Information Policy Research (FIPR) is an independent body that studies the interaction between information technology and society. Its goal is to identify technical developments with significant social impact, commission and undertake research into public policy alternatives, and promote public understanding and dialogue between technologists and policy-makers in the UK and Europe.

FIPR would like to congratulate the Secretary of State and his team on his consultation document on NHS IT, 'An Information Revolution', which in our view is a much-needed breath of fresh air. After the mistakes of the last twenty years' NHS IT, from the IM&T Strategy of the early 1990s through NPfIT, at last we have an IT strategy whose focus is the records kept by providers to support care rather than collection of data by the centre.

In our view, the strategy is 80% right. In what follows we try to point out some things that could be improved and some potential traps along the road to implementation.

To help put things in context, we are releasing as an annex a previously unpublished briefing paper written in 1997 for the incoming Labour government, as a reminder of how little has been achieved since then. Its advice is valid today; if only ministers had paid attention! The opportunity costs to health in Britain have been significant; centralised mismanagement has done serious damage to Britain's healthcare IT industry, which hopefully can now start to regain its former world-leading position.

Functionality

Subject to constraints set by considerations of safety and privacy, which we will discuss in the next section, the objective should be a dramatic improvement in the functionality available to the care teams treating patients directly. This can only be achieved if clinical systems are specified and purchased by providers rather than by the centre. GP systems work well, as (until recently) they were bought by GPs using their own money, and thus did what GPs needed. By comparison, centrally-procured systems worked badly if at all; their functionality reflected the many (often conflicting) priorities of the centre. The single biggest gain available from this reform is to let people buy the systems that help them best get their work done, and restricting the centre to ensuring interoperability based on open standards, which should be European standards rather than national ones where possible. Decentralisation is long overdue, and can bring great gains. We welcome it.

That said, we are concerned that many of the questions in the consultation document appear to nudge policy quietly back towards centralisation. To take a relatively innocuous

example, it would be convenient if GPs would accept repeat prescription orders by email rather than expecting patients to walk to the surgery; and indeed some practices already do. If the consultation respondents came down in favour of this, what will the Department do? Will it procure a central email system for repeat prescriptions? Will it put patient email support into a future RFA for GP systems? Will it mandate practices to turn round patient email, perhaps under QOF? The decentralised approach is to let patients move to GPs who give good service, and move more of their funding back to capitation.

Patient Access to Records

The principle of "no decision about me, without me" is laudable; medical treatment almost always requires informed consent and in general the more informed this consent is the better. There are also opportunities for people to improve their health using online systems that help them achieve health targets by monitoring diet, exercise and so on, However it is wrong to jump from there to the conclusion that making all medical records available online to all patients is relevant, needful or even wise.

First, the Greenhalgh report demolished the argument that patients want access to their records, as proposed in section 2.8. Second, such access is hard to do safely because of the problems of coerced access, particularly to the records of children, abused women and other vulnerable patients, and because of the risks arising from malware-infected PCs, shared PCs and deceptive web services. Third, a policy decision to compel online access to health records leads to a drive to acquire central copies of health records so that the policy can be implemented via government websites rather than left to GPs (many of whom would quite properly drag their heels or even ignore it on safety and ethical grounds). It would thus allow the centralisation agenda back in through the back door.

Patient control of their records is a very worthwhile aim, and indeed a requirement of human-rights law. However it must not be taken to mean the forcible collection of patient records to a government website, but something completely different. To understand what, we have to consider safety and privacy.

Safety and Privacy

Since its inception in 1998, FIPR has been engaged with the safety and privacy of personal health information. We wrote several relevant reports, most notably 'Database State' in March 2009 [1], which pointed out that a number of the central systems built by the previous Government were contrary to human-rights law. While in opposition, the Conservatives and Liberal Democrats each promised to abolish some of the systems named and shamed by "Database State". The Coalition Government has formally abolished some of them, including the ContactPoint children's database.

NHS systems have been the greatest source of reported privacy breaches in the UK since the HMRC debacle made such breaches salient in 2008. One of the systems identified in the "Database State" report as almost certainly in breach of human-rights law following the I v Finland case is the Secondary Uses Service, SUS. As patients generally have the

right to restrict their personal health information to the clinical teams treating them, it is unlawful for the government to retain sensitive personal information for secondary uses without their consent. At the very least this means that patients who wish to opt out of having their data kept for secondary purposes must be able to do so. This in our view is the correct interpretation of “putting patients in control of their data”. It is not only European law, but also in line with patient preferences as expressed in a significant number of opinion surveys (e.g., [2] [3]).

The issues are not restricted to secondary uses, but affect care records directly. An unpleasant legacy from NPfIT is that a number of care providers are unable to provide care without sharing records outside the care team, thanks to increasing reliance on hosted, shared and other remote systems. In one well-known case, the activist Helen Wilkinson has been unable to get NHS treatment without having her information shared outside the care team; there are other cases.

Privacy breaches cause serious harm to individuals and place their lives directly at risk. For example, we are aware of an ongoing lawsuit by a woman who was seriously assaulted and injured by her ex-husband after he found her address from a relative who was a ward clerk at a trust. Neither the woman's GP nor A&E knew how to stop-note her on PDS, or even that it might have been a good idea to do so.

We draw the Department’s attention to the UK Government's Business Impact Level Tables that appear within HMG Information Assurance Standard No 1. The only realistic debate about PDS is whether its compromise may “threaten life directly leading to limited loss of life” – Business Impact Level 5, with a minimum mandatory classification of SECRET – or merely lead to "serious risk to any individual's personal safety (e.g. the compromise of the address of a victim of abuse, where serious further abuse is likely if such information became known)" is considered Business Impact Level 4, with a minimum mandatory classification of CONFIDENTIAL. And the tables refer to a single record, while PDS contains the records of tens of millions of people: because of this aggregated risk, it should be classified SECRET. The NHS is required to apply a commensurate level of security. By treating PDS as unclassified and permitting access by hundreds of thousands of people who have not been properly vetted or indoctrinated, the Department of Health has negligently disregarded official advice on information assurance. Similar considerations apply to many other central systems.

One final remark needs to be made about safety and privacy. That is that the operators of some health systems, such as SUS, appear to hope that anonymisation will get them off the human-rights hook. This hope is vain. While anonymity can be used to protect privacy in some tightly-defined applications (such as the IMS prescription system that was the subject of the Source Informatics judgement) it does not work in general – as recognised by the Caldicott Committee many years ago. Where records contain postcode plus date of birth, or even where they link a number of episodes affecting the same person, re-identification is usually easy; see [4] [5].

Conclusion

The consultation contains much that is welcome. The excessive centralisation of NHS computing has imposed significant real and opportunity costs on health providers and it is time to let them buy whatever systems will, in their opinion, enable them to deliver care better. Systems tend to advance the interests of whoever pays for them; systems whose job is to support doctors must once more be bought be doctors. That alone will deliver the "Information Revolution" that the NHS needs. The role of the centre should be limited to ensuring interoperability. The Department's move in this direction is long overdue and holds out the prospect of significantly increasing the efficiency and safety of healthcare provision while promoting innovation and health IT employment.

However, it is time to tackle the safety and privacy problems about which the NHS has been in denial for over a decade. First, both public opinion and European law demand that patients should be able to restrict their personal health information to the clinical teams who are treating them. Systems bought henceforth must not be designed so as to make this impractical. Second, the central systems that will remain (such as PDS) need to be properly protected, because of their demonstrated potential to threaten life directly when abused. The information on such systems must be classified in accordance with existing CESG guidance – at least CONFIDENTIAL, and in some cases SECRET. This will ensure that careless or dishonest staff who cause serious harm by leaking personal information will face prosecution under the Official Secrets Act and a prison term.

Ross Anderson FRS FREng
Foundation for Information Policy Research
Cambridge, December 2010

References

[1] Ross Anderson, Ian Brown, Terri Dowty, Philip Inglesant, William Heath, Angela Sasse, *Database State*. Joseph Rowntree Reform Trust, 2009

[2] Alan Hassey, Mike Wells, Clinical Systems Security – Implementing the BMA Policy and Guidelines, *Personal Medical Information – Security, Engineering and Ethi*cs, 1997

[3] Victoria Armstrong, Julie Barnett, Helen Cooper, Michelle Monkman, Public Perspectives on the Governance of Biomedical Research: A qualitative study in a deliberative context, Wellcome Trust 2006

[4] Paul Ohm Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 UCLA Law Review (2010).

[5] Ian Brown, Lindsay Brown, Douwe Korff, Using NHS patient data for research without consent, Law, Innovation and Technology, 2(2) (2010), pp 219–258