

Patients will resist medical record sharing if NHS bosses ignore their privacy fears

August 19 2015, by Eerke Boiten



Credit: AI-generated image ([disclaimer](#))

Can it really be that giving pharmacists access to their customers' prescription information, even those pharmacists based in a supermarket, is viewed as a problem? After all, when done so using their professional credentials and code of conduct, with your explicit permission to do so, it seems an example of sensible data sharing.

But in England in 2015, this [exact scenario](#) has been reported as "[Now Tesco has access to your medical records](#)", with the implication the medical data will be used for marketing purposes. This looks like a serious overreaction – even though there are [justified concerns](#) about the introduction of this scheme and its operational processes.

One particular centralised NHS patient database is called the [Summary Care Record](#), from which this particular use of medical data is drawn. There are some [uncertainties](#) on what data is included now and in the future, and on what consent patients have given. But these are not nearly as substantial as the many problems that already surround the – entirely different – care.data database.

And that is the problem: the painful, two year saga over care.data has significantly eroded public trust in NHS England and in the government's capacity to treat people's [medical records](#) responsibly and competently. Not nearly enough has been done to regain that trust before embarking on other ill-defined schemes.

No lessons learned

On the contrary, only this June the government sought to access [GP appointment data](#) including sensitive details, bypassing GPs and patients and instead going directly to the medical systems suppliers. The backlash on this move was effective and a U-turn rapidly followed, but it confirmed what many already suspected about the government's cavalier attitude to medical confidentiality.

NHS England, meanwhile, has been running a year-long propaganda campaign for [care.data](#). The Department of Health's latest quango, the [National Information Board](#), has just finished [a series of public meetings](#), in which they have also been commenting on the care.data fiasco. A "failure to communicate the benefits" is apparently still the [explanation](#) –

no progress there then.

Competence and good intentions

[Rebuilding trust](#) is not easy, and it never happens fast. The public needs to be convinced of both competence and honourable intentions within NHS authorities and the government.

So far, both are lacking. The fiasco of the NHS National Programme for IT, finally [abandoned in 2011](#) at a cost of billions, still resonates in the people's minds. Major data breaches are still too frequent, including of [medical data](#), and thus security worries have only added to the existing doubts in this area.

The [Partridge report](#) in 2014 on NHS data sharing identified weak procedures and sloppy practices, concluding that "it is not clear if data has been released for appropriate purposes in all cases". Following the scandal in 2014 where [medical data was sold to insurance firms](#), tighter definitions of "appropriate purposes" had been expected. Instead, by limiting such use to "[the promotion of health](#)" in the [2014 Care Act](#), the government has made only the most vague constraints on data sharing. In terms of convincing the public of their respect for privacy, this was a missed opportunity.

Reports from the Health and Social Care Information Centre, which manages access to NHS data for third parties, show [data continuing to flow to commercial customers](#) such as data brokers and analytics companies. It's unclear how this satisfies the principle that there should be "[no surprises](#)" for patients in how their medical data is dealt with.

Rebuilding trust with patients

While the appointment of Lady Fiona Caldicott as the [national data guardian](#) should have been a major step forward, even this has been undermined by the postponement of the legal basis for her role, and the fact that the [52 questions](#) she'd demanded answers from the government regarding care.data in 2014 remain unanswered.

Ultimately, what NHS England and the UK government should do is to face privacy and security risks head-on. Newspaper headlines and the public's response reveal that these are not just the concerns of fringe privacy campaigners, worries that stand in the way of great health research and public service efficiencies. People are rightly concerned about where their [medical data](#) goes, and it's about time the government and NHS authorities shouldered the responsibility of listening and doing something about it.

This story is published courtesy of [The Conversation](#) (under Creative Commons-Attribution/No derivatives).

Source: The Conversation

Citation: Patients will resist medical record sharing if NHS bosses ignore their privacy fears (2015, August 19) retrieved 10 May 2024 from <https://medicalxpress.com/news/2015-08-patients-resist-medical-nhs-bosses.html>

| |
|---|
| This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only. |
|---|