Oxford

helen.salisbury@phc.ox.ac.uk Follow

Helen on Twitter: @HelenRSalisbury

Cite this as: *BMJ* 2021;373:n1451<http://dx.doi.org/10.1136/bmj.n1451>

Published: 09 June 2021

PRIMARY COLOUR

Helen Salisbury: Should GPs break the law on data privacy?

Helen Salisbury *GP*

NHS Digital plans to extract all data coded in GP held medical records in England, unless patients opt out first. These data include all physical and mental health diagnoses, physiological measurements, test results, and medications. The data will be pseudonymised, meaning that identifiers such as name, NHS number, date of birth, and the second part of the postcode will be hidden—but NHS Digital has a key to re-identify records, which it will do “where there is a legal reason.”

The stated aim of the dataset is to assist research and planning. The list of organisations NHS Digital may share data with includes other government departments, universities, charities, research bodies, and drug companies. NHS Digital says that it only ever releases the minimum dataset necessary and is confident that it has robust systems in place to prevent breaches of confidentiality. However, not everyone is reassured, as re-identifying people from an incomplete dataset is a developing art and is likely to evolve further.¹ The Information Commissioner's Office is clear in its most recent guidance that pseudonymised data are therefore personal data.²

Leaving aside the question of whether absolute data security can be guaranteed, a more fundamental question concerns consent. General practices are legally obliged to transfer data to NHS Digital under the 2012 Health and Social Care Act, but how does this square with my ethical obligation to my patients? Some will be content to have their data used for research, as proposed, and some will not, but there are clear implications for trust in future consultations if this happens without their knowledge. They consult with me with a presumption of confidentiality, and they don't expect me to share their medical information without their consent. There's something sacrosanct about a medical consultation, with similarities to a religious confessional: whatever they tell me, unless there's a risk to others, I don't break my patients' confidentiality.

This project has been in development for three years, but the details were released only on 12 May, with a 23 June deadline for patients to opt out (now delayed until September). Communicating this complex issue has been left entirely to GPs, many of whom are only now finding out about it themselves. This contrasts starkly with direct-to-patient communications about covid-19, which have been handled centrally, or the care.data fiasco of 2013, when letters were sent to every household.

Why the secrecy? This opt-out system presumes consent—and that's a very bold presumption. For consent to be valid, one must be confident that patients have had adequate opportunity to learn

about the proposal and to exercise their choice. This is clearly not the case here, and GPs are left in a difficult position.

One option would be to apply an opt-out code to all patients on our lists, inviting them to opt back in again if they wished. Alternatively, we could delay sharing data until we're satisfied that all of our patients are adequately informed. Both of these actions would be in breach of the law as it stands—so the question is, do we break the law, or do we break faith with our patients?

Competing interests: See www.bmj.com/about-bmj/freelance-contributors.

Provenance and peer review: Commissioned; not externally peer reviewed.

- 1 Brogan C. Anonymising personal data “not enough to protect privacy,” shows new study. Imperial College London. 23 Jul 2019. <https://www.imperial.ac.uk/news/192112/anonymising-personal-data-enough-protect-privacy/>.
- 2 Information Commissioner's Office. Introduction to anonymisation: Draft anonymisation, pseudonymisation and privacy enhancing technologies guidance. May 2021. <https://t.co/386jj7rKoT?amp=1>.