Editorials

The use of NHS patient data:

report by the National Data Guardian for Health and Care

The recent report by the National Data Guardian for Health and Care (or 'Caldicott 3') reviewed NHS data security, consent, and opt-outs for patients.[1]

At the same time the Care Quality Commission (CQC) was also asked to review current approaches to data security across the NHS.[2] As soon as both reports were published, care.data (NHS England's controversial data-sharing programme) was immediately closed down.[3]

CALDICOTT 3

There is little doubt that the use of large-scale health data has considerable potential to benefit not only patient care but also public health and research.[4] The use of such data, however, raises great concerns about data security, patient privacy, and probably most importantly public trust, not only in the NHS but also in the relationship with their doctor. The demise of care.data was in no small part due to a loss of public trust and Caldicott 3 demands increased dialogue with the public to restore their trust. The NHS and GPs in particular, must be 'beyond reproach' in their use of health data to improve both direct and indirect patient care as well as contributions to public health and health research. Dame Fiona Caldicott's review follows her previous reviews in 1996/1997 and 2013. The first of her reviews recommended six principles for the protection of people's confidentiality (the Caldicott principles) and the second recommended an additional Caldicott principle which stated that duty to share information can be just as important as the duty to protect patient confidentiality. Caldicott 3 addresses the further issue of data security and future models of consent.

As far as data security is concerned, the new Caldicott report sets out 10 standards which need to be applied in every healthcare organisation to address the three causes of data breaches: people, processes, and technology. As a way of improving confidence and trust in data security, Caldicott also calls for tougher sanctions for malicious breaches and the government plans to introduce criminal penalties for people who deliberately use anonymised data to re-identify individuals.

CQC REVIEW

The CQC review[2] published at the same time sets out new data security standards which are intended to be applied across all health and social care organisations, although further work will have to be undertaken to establish the validity of these standards for organisations providing social care. The CQC recommendations emphasise the importance of leadership in demonstrating clear ownership and responsibility for data security. Other recommendations from the CQC review include a removal of outdated computer systems and emphasise the importance of providing all staff with the right information, tools, training, and support to allow them to do their jobs effectively while still being able to meet their responsibilities for handling and sharing data safely. The CQC review also calls for a review of the arrangements for internal data security audit and external validation. However, these recommendations put general practice in an anomalous situation because we do not purchase our own IT systems and are dependent on others but answerable to CQC (and the Information Commissioners Office) for any failings. In addition, we will still have a responsibility to guard against direct cyber attacks (for example, botnet viruses) as well as other causes of data breaches involving people, processes, and technology.

"... GPs in particular, must be 'beyond reproach' in their use of health data ..."

A NEW CONSENT MODEL

The recent Caldicott review proposes a new consent or opt-out model that describes clearly when information is used and when patients have a choice to opt-out of their personal confidential data (PCD) being used. This may be the 'last chance saloon' for the use of big data by the NHS. Care.data failed as a result of poor communications, weak governance processes, and an unclear opt-out mechanism.[3] Caldicott proposes an 8-point model which guarantees the right to opt-out of your personal confidential information being used for other purposes beyond your direct care. The opt-out covers:

- PCD being used to provide local services and run the NHS social care system (for example, to find out patients' experience of care and treatment for cancer).
- PCD being used to support research and improve treatment and care (for example, research determining the effectiveness of the NHS bowel cancer screening programme).

This opt-out can be presented as either two separate opt-outs or there could be a single opt-out covering PCD being used for the running of the health and social care system, and to support research and improve treatment and care. Under Caldicott 3 it will only be necessary to state your preference once and there will be an opportunity to change your mind.

Explicit consent will continue to be possible even if you opt-out, whereby you can continue to give your own explicit consent to share your PCD if you wish; for example, to contribute to a specific research study. However, and this is key to Caldicott 3, the opt-out will not apply to PCD, which in future will flow directly to the NHS Health and Social Care Information Centre (HSCIC), now known as NHS Digital. Alternatively, it would be possible to use pseudonymisation–at-source and rely on 100% accuracy and completeness of NHS number records but this is unlikely given the current position of the pseudonymisation review. Indeed, linkage and anonymisation could be easier, more effective, and secure if the NHS was willing to invest in enforcing the use of the NHS number since, if providers are going to have to develop systems that will read the central opt-out record, why cannot the NHS number be read at the same time?

NHS Digital will act as the statutory 'safe haven' for the health and social care system and anonymise the PCD which it holds, sharing it with only those that are authorised to use it. By using these anonymised data, NHS managers and researchers will have less need to use people's PCD and indeed little justification for doing so. It is also important to note that the opt-out will not apply where there is a mandatory legal requirement or over-riding public interest; for example, in areas where there is a legal duty to share information; such as, an NHS fraud investigation.

"The benefits to patient care, public health, and health research outweigh the small risks to data security and patient confidentiality ..."

PUBLIC TRUST

At the time of writing the government response to Caldicott 3 is still awaited. There is little doubt, however, that there is currently a low awareness of how data are used not only by the public but also by healthcare professionals within the NHS.[5] Apart from this difficulty in ensuring that the public and professionals are fully informed about these complex proposals, there are other challenges to implementing them (for example, people need to know exactly what it is they are 'opting out' of). These include the poor record of NHS Digital in controlling data flow out of the centre[6] and what is to be done about the more than 1 million people who registered objections to the care. data and wished to opt-out of the system? There are also questions about the future of national audit programmes such as the existing one for diabetes care. In addition, there is no doubt that considerable support will be needed for practices if the new data security requirements are to be adopted and patients to be fully informed. GPs are by far and away the most trusted of all health professionals within the NHS and nothing should be done to jeopardise that existing trust.[7] Such trust must not be abused if and when Caldicott 3 is implemented. Communication with patients is critical for success and although GPs will continue to have a legal duty as data controllers, the new proposals remove this responsibility with regard to the flow of data from practices direct to NHS Digital.

Although there may indeed be low awareness by health professionals and the public of how their data are used within the NHS, the more informed people are, the more likely they are to approve of health data being used for other purposes, provided there was clear public benefit, although most would object strongly to the use of any kind of health data by insurance and commercial interests. Most reasonable people using the NHS, however, would expect that their data can be used to not only monitor outcomes of their treatment to improve the quality of care, but also that new interventions can be properly evaluated and implemented to improve health care. Therefore, it is essential that an appropriate and ethical way to use NHS data for these purposes is found and the new Caldicott report provides a way forward to do this.[8,9] It is not an impossible task, the systems for doing this have already been implemented elsewhere. The Welsh Secure Anonymous Information Linkage (SAIL) contains a large number of data sets and a platform for sharing knowledge about using the data and successfully operates a remote access system providing secure data access from approved users and data analysis tools.[10] Similarly, the Scottish Health Informatics Programme (SHIP) has also developed ways for its researchers to manage and analyse electronic patient records and associated linked data. It achieved this by a substantial public engagement programme to determine the public's preferences, interests, and concerns about the use of health data for research as well as their acceptance and attitudes towards the aims of the programme. This has enabled a transparent and publicly acceptable approach to governance of research with health data.[11]

In the final analysis, Caldicott 3, if adopted, reduces the current opt-out opportunities for patients. The most important thing, however, is trust and engagement and Dame Fiona's report provides a way forward. The benefits to patient care, public health, and health research outweigh the small risks to data security and patient confidentiality and her clear, rational approach should be supported despite the challenges of implementation.

Nigel Mathers,
Honorary Secretary, RCGP, London, and Professor of Primary Medical Care, Academic Unit of Primary Medical Care, University of Sheffield, Sheffield.

Ralph Sullivan,
Clinical Lead, RCGP Patient Online, RCGP Clinical Innovation and Research Centre (CIRC), London.

Arjun Dhillon,
Vice-Chair, Health Informatics Group, RCGP, London.

Imran Rafi,
Chair of CIRC, RCGP Clinical Innovation and Research Centre, London.

Amelia Bell,
Senior Workforce Policy and Research Officer, RCGP, London.

ADDRESS FOR CORRESPONDENCE

Nigel Mathers
Academic Unit of Primary Medical Care, University of Sheffield, Samuel Fox House, Northern General Hospital, Herries Road, Sheffield S5 7AU, UK.

Email: n.mathers@sheffield.ac.uk

Provenance
Freely submitted; externally peer reviewed.

DOI: https://doi.org/10.3399/bjgp17X688933

REFERENCES

1. National Data Guardian for Health and Care. *Review of data security, consent and opt-outs*. 2016. https://www.gov.uk/government/publications/review-of-data-security-consent-and-opt-outs (accessed 10 Jan 2017).
2. Care Quality Commission. *Safe data, safe care. Report into how data is safely and securely managed in the NHS*. 2016. http://www.cqc.org.uk/sites/default/files/20160701%20Data%20security%20review%20FINAL%20for%20web.pdf (accessed 10 Jan 2017).
3. NHS England. The care.data programme. https://www.england.nhs.uk/ourwork/tsd/care-data/) (accessed 10 Jan 2017).
4. Van StaaT-P, Goldacre B, Buchan I, Smeeth L. Big health data: the need to earn public trust. *BMJ* 2016; **354:** i3636.
5. Ipsos MORI. *The one-way mirror. Public attitudes to commercial access to health data*. 2016. https://www.ipsos-mori.com/researchpublications/publications/1803/Commercial-access-to-health-data.aspx (accessed 10 Jan 2017).
6. Partridge N. *Review of data releases by the NHS Information centre*. 2014. www.gov.uk/government/uploads/system/uploads/attachment_data/file/367788/Sir_Nick_Partridge_s_summary_of_the_review.pdf (accessed 10 Jan 2017).
7. OPM. *Review of public and professional attitudes towards confidentiality of healthcare data*. 2015; http://www.gmc-uk.org/Review_of_Public_and_Professional_attitudes_towards_confidentiality_of_Healthcare_data.pdf_62449249.pdf (accessed 10 Jan 2017).
8. Mathers N, Watt G, Perrin N. *Towards consensus for best practice: use of patient records from general practice for research*. 2009. https://wellcome.ac.uk/sites/default/files/wtx055661_0.pdf (accessed 10 Jan 2017).
9. Nuffield Council on Bioethics. *The collection, linking and use of date in biomedical research and health care: ethical issues*. 2015. http://nuffieldbioethics.org/wp-content/uploads/Biological_and_health_data_web.pdf (accessed 10 Jan 2017).
10. Jones KH, Ford DV, Jones C, *et al*. A case study of the Secure Anonymous Information Linkage (SAIL) gateway: a privacy-protecting remote access system for health-related research and evaluation. *J Biomed Inform* 2014; **50:**196–204.
11. Scottish Health Informatics Programme. 2012. *A blueprint for health records research in Scotland*. 2012. www.scot-ship.ac.uk/sites/default/files/reports/SHIP_BLUEPRINT_DOCUMENT_final_100712.pdf (accessed 10 Jan 2017).