Newchurch

Caldicott 2016 – A Simpler Approach to Consent?

A Newchurch Paper

September 2016

Since its foundation in 1983 Newchurch has published a series of occasional papers on key issues in the health and care sector. This latest paper provides an analysis and commentary on the National Data Guardian's report, *Review of Data Security, Consents and Opt Outs* published in June 2016. This Review puts forwards a series of recommendations for how the health and social care sector should allow individuals to object to the sharing of their personal confidential data. These recommendations may have a significant impact on the access that care professionals have to an individual's data and on the ability of an individual to control the use of their data, they are however unlikely to be the final answer in an extremely complex and confused debate.

The author **Kingsley Manning** founded Newchurch Limited in 1983 and was latterly Executive Chairman of Tribal Health and a Senior Advisor at McKinsey & Company. From May 2013 until June 2016, Kingsley Manning was Chair of the Health and Social Care Information Centre (NHS Digital), the Department of Health's arms-length body responsible for data and technology across the health and social care sector.

Caldicott 2016 – A Simpler Approach to Consent?

Published in June the latest Review undertaken by Dame Fiona Caldicott[1] proposes a new model of opt-outs and consents with respect to who may have access to an individual's personal confidential health and care data. The Review, prompted by the Care.Data debacle, was undertaken in a matter of months and was constrained by the predetermined requirement established by the Secretary of State for a 'simple' solution. Despite the considerable efforts of Dame Fiona and her team, the proposals which are now subject to consultation are unlikely to settle the complex issues surrounding data privacy and may well add yet another layer to an already extremely confusing picture. Ultimately the 'simple' solution sought by the Secretary of State, which individuals and care professionals could both understand and trust, is unlikely to be achieved as a result of this Review. What is really needed is a complete overhaul of the web of policy, statute and law that overwhelms the subject. But such an overhaul is very unlikely given the government's other priorities, the Department of Health's lack of expert resources, the caring profession's conflicting interests, the demands of the research industry and the daunting immediate prospects facing the NHS.

How did we get here?

The need over more than 20 years for repeated attempts to clarify who can see and use an individual's personal confidential data, reflects in part the rapid developments in technologies and shifting public attitudes. There has also been consistent pressure from care professionals, researchers and administrators to have increasing access to the expanding data assets. Thus over two decades there have been numerous statutory attempts at resolution, including the Data Protection Act, The Medicines Act 2002, The Health and Social Care Act 2012, and The Care Act 2014, which are all set within the evolving common law framework and the principle of respecting personal confidentiality. Alongside the legislative initiatives there have been two previous Caldicott Reviews and many statements of policy, including in the NHS Constitution and various position statements by Secretaries of State. These statements include those in September 2013 by the current incumbent, which set out how patients could object to their information leaving their GP or being passed on by the Health and Social Care Information Centre, the Department of Health's arms length body with primary responsibility for collecting and disseminating health data.

[1] National Data Guardian for Health and Care – *Review of Data Security, Consent and Opt-Outs – June 2016*

As a result, all the available evidence, including that provided by the latest Caldicott Review, suggests that pretty much everyone is confused. Health and care professionals and individual citizens alike do not understand what data there is, how it used and their mutual obligation and responsibilities with regard to confidentiality.

This confusion is well illustrated by the public reaction to the care.data programme and the general surprise as to where some of '*their*' data was going to. As a result more that 1.2 million people 'opted-out', refusing access to their data by NHS administrators, planners and researchers; an opt-out that was not implemented for nearly two years, by which time the care.data programme had been suspended and subsequently cancelled.

Terms of Reference

In an admirable attempt to respond to the confusion, the Secretary of State announced the current Caldicott Review in September 2015. In doing so he would also have been aware not only of the problems generated by the care.data programme but of a range of challenges as to the collection, and use of personal confidential data. Within the NHS there is continuing uncertainty as to the legal basis for the use of personal confidential data by NHS England and Clinical Commissioning Groups and by the various integrated care initiatives that have been established across the country. These initiatives have further fuelled the frustration of many Local Authorities seeking to gain access to health data. And within central government there is a continuing initiative, driven by the Cabinet Office and leading to the recently published Digital Economy Bill, seeking to promote much greater data sharing across the whole of government. In the eyes of some, the Department of Health has been a reluctant partner in increasing access to health data, for the greater good of government and the wider economy.

The Secretary of State's Terms of Reference to Dame Fiona were therefore to propose a new consent/opt-outs model for data sharing. *To develop a single question consent model which makes it absolutely clear to patients and users of care when health and care information about them will be used, and in what circumstances they can opt-out.*

And the work was to be completed in three months.

The Process

Within these constraints Dame Fiona and her team achieved a great deal. Within the limited time available much of the evidence base was drawn from a series of interviews, focus groups, workshops and 'policy labs' held over a three month period.

Given the time constraints there are of course significant omissions. There is no examination or definition of the nature of the problem, nor of its scale. There is no analysis of the weaknesses of the current system or of the impact of those weaknesses. Conversely there is no analysis of the possible benefits of the proposed solutions or of any associated risks.

There is no discussion of possible technical solutions nor of the technical viability of the recommended solutions. And typical of reports concerned with the NHS there is no consideration of how other sectors or indeed other healthcare systems deal with similar problems. As ever the NHS is viewed from within its unique bubble. The rapidly evolving world of personally generated and controlled data, of the world of Facebook and Google, of generations assuming almost infinite access and dissemination of data and information, doesn't get a mention.

The Recommendations

The Review's recommendations can be grouped into three areas; the first deals with the sharing of personal confidential data for direct care and the second with the use of anonymised and deidentified data for purposes other than direct care, often referred to as the secondary use of data. The final group of recommendations deal with the use of personal confidential data; that is data which allows the individual to be identified, again for secondary uses, such as management, planning and research.

Personal Confidential Data for Direct Care

The Review does not make any major recommendations that seek to change the current position on the use of personal confidential data for direct care. Health and care professionals have a duty to share relevant data where this will benefit an individual and there is no requirement to seek an individual's consent for so doing. Although individual's can object to their information being shared and whilst individuals should never be 'surprised' that their data has been shared.

The Review does not therefore propose a general opt-out with respect to personal data being shared when a care professional deems it appropriate to do so for the purposes direct care. In general this must be right, assuming as it does an essential bond of trust between the carer and cared for. What the report does reiterate is that an individual's consent must be obtained before the whole health record is shared, for example when a GP wants to pass an individual's complete GP record to another care provider.

As it stands, however, an individual has no way of knowing or indeed a clearly defined right to know, whether their data has been shared when it should have been or whether or not it has been used appropriately. The Review makes no recommendations for audit, or for traceability, nor recommendations as to how an individual might find out where their data has gone and who has seen it.

A significant change that the Review does propose is that risk stratification, the use of algorithms primarily applied to health data to identify individuals with elevated risks with respect to specific diseases or conditions or in support of integrated care programmes, should be reclassified as direct care. If this recommendation is implemented it would become permissible to use an individual's personal confidential data, for the purpose of risk stratification, without that individual's consent or knowledge. The logic here appears to be that such analyses are inherently and always, in the best interest of the individual.

However such analyses are both poorly regulated and often unproven. In a recent case an algorithm used for predicting the risk of heart disease for hundreds of thousands of patients was found to be wrong. The presumption as to the best interest of the individual is also open to question. Local authorities are very interested in using health data combined with social care date and other datasets they have access to, to identify individuals and families who are or potentially will be expensive consumers of scarce resources. In these cases early interventions might be deemed by the professionals as in the best interest of the individual and their family, but the recipients of any resulting intervention, based on accessing their data without their knowledge or agreement, might take a very different view. There is the potential danger, that particularly vulnerable groups may withdraw from the formal care system to avoid such surveillance.

A further danger is that using risk stratification, algorithms, for case finding may also be part of a process of case exclusion. Unknown to an individual, he or she may be identified as unsuitable for a particular treatment, by virtue perhaps of being too ill, too old or too expensive.

Anonymised and Deidentified Data for Secondary Uses

The general position taken by the Review is that individuals should not be able to object, to 'opt-out' of their anonymised and deidentified[2] data being used for purposes such as research, regulation, commissioning and service planning. The argument being that once data is deidentified in-line with the standards set out by the Information Commissioner, then the link between the individual and 'their' data has been broken.

[2] Data where key fields have been removed so that an individual cannot be identified from the remaining data alone

Recognising that there is the possibility of reidentification, particularly through linking multiple data sets, the Review recommends the rigorous application of the existing legal sanctions against such practices and their potential extension to include criminal penalties.

This approach seems reasonable both with respect to the management and regulation of NHS services and in support of research. The Review rejects the notion of a social contract between service users and the NHS, a contract implying an obligation on service users to share their data with the NHS. However given the practical needs of running the NHS and its basis as a community funded, shared risk system, the requirement to share deidentified data is a reasonable requirement for beneficial participation. Whilst there are risks in sharing deidentified data, and some will object on principle, the proposed approach balances these appropriately against the general good for the community as a whole.

The important innovation that the review does recommend is that there should be a single-source of deidentified data, the Health and Social Care Information Centre, renamed NHS Digital. It will not be possible for an individual to have a general opt-out of their data being passed from their service provider to NHS Digital, which will then provide deidentified data to all users, in accordance with its existing statutory responsibilities. Such disseminations are subject to contract, independent advice, the provisions of The Care Act 2014 and full public scrutiny.

Personal Confidential Data for Secondary Uses

It is with respect to the secondary use of personal confidential data that the Review makes its most important recommendations and seeks to meet the challenge set by the Secretary of State. Currently the use of such sensitive personal data is subject to a wide range of legal restrictions and requirements. There appears to be no recommendation or intention for any of these restrictions or requirements to be changed.

Dame Fiona will have been under considerable pressure to normalise the current awkward and temporary arrangements under which commissioners and commissioning support users are gaining access to personal confidential data. The Review however, specifically declines to extend access to personal confidential data by NHS commissioners, beyond that allowed under existing legislation. Instead the Review recommends that greater use should made of deidentified to be provided by NHS Digital. So that if the Review's recommendations are implemented commissioners and commissioning support units will still need to establish a specific legal basis for accessing personal confidential data, for example by gaining approval from the Confidentiality Advisory Group (CAG) or through individual informed consent.

Alongside research the Review identifies an array of purposes, including public health, regulation and monitoring, for which a range of primarily statutory bodies[3], have argued that they require personal confidential data. The argument excepted by the Review is that these purposes are legitimate, allowed by statute, and that the practical difficulties of dealing with multiple 'informed consents' or 'opt-outs' from the general population are too great.

The solution proposed is for a single, national opt-out model, which would be registered once but apply to the whole system, including the statutory bodies. The Review suggests either a one or two question approach. In the single question version an individual would be able to opt-out from their personal identifiable data being shared for any purpose, including research, even when there is an existing legal basis for the use of that data. In the two question version the individual could opt-out of sharing their data with statutory bodies but not for research and visa-versa.

Once an individual has 'opted-out' in theory at least, no organisation within the NHS and social care system will share their personal confidential data. However the list of exemptions is considerable, including where there is a mandatory legal requirement or '*..an overriding public interest'*. And there is specific exemption proposed for the passing of data to NHS Digital and its use by NHS England and Clinical Commissioning Groups for invoice validation.[4]

Even though an individual has registered a general opt-out they would still be able to give 'informed consent' for a specific use of all or part of their data. For example an individual could agree to participate in a particular research project whilst maintaining a general opt-out.

The ability to make a general 'opt-out' will be welcomed by many individuals concerned to have greater control over the use of their personal confidential data, even with the considerable list of exemptions. Making such an 'opt-out', most likely through a single, national electronic portal, will require a positive action on the part of an individual.

Where a patient does not 'opt-out' this does *not* mean that that they will have consented to the secondary use of their personal confidential data. Any organisation wanting access to that data would still either have to gain specific 'informed consent' or establish some other legal basis.

[3] The principle statutory bodies are NHS England, Public Health England, the Care Quality Commission, Clinical Commissioning Groups, and Local Authorities.

[4] Invoice validation is the process whereby NHS commissioners, as payors, are able check the details and accuracy of any invoice presented to them by a service provider.

As a result the care professional, manager and researcher will be faced with two groups within the general population. Those whose position is relatively clear, who have 'opted-out' but who can agree to share their data for specific purposes and the remainder who have not 'opted-out' but whose personal confidential data can only be used either with 'informed consent' or where there is another legal basis.

The default position, assumed by the Review to be supported by the majority of the population, will be to do nothing; that most individuals will not 'opt-out'. Given that individuals will not be prompted to consider an opt-out or given any information as to how their data has been, is, or will be used, it is possible that the great majority of the population will take no action.

There are however, no recommendations as to audit and traceability; how an individual can find out what data there is and who has seen it. Whilst there will be a single portal for registering an 'opt-out' there will be no simple or single source of information where an individual can see where they have given consent, or where their data has been used on the basis of 'implied consent' or through the establishment of an appropriate legal basis. Many individuals might be surprised to find that their personal, identifiable, confidential data has been used, quite legally, but without their knowledge, for a range of audit, regulatory and research purposes.

This is not the end of the data privacy debate

The third Caldicott Review, as with its predecessors, makes a number of important and helpful recommendations. The proposals with respect to NHS Digital becoming the single-source for deidentified data and the presumed default use of such data by commissioners and statutory bodies, should significantly reduce the use of personal confidential data and with it the risks of data breaches and misuse. Similarly the creation of a single, general opt-out covering the use of personal confidential data for secondary purposes is an important step forward. Together these proposals are a significant step forward in meeting the concerns of a substantial minority of the population

However what is being proposed is not a simplification of the existing system, all of which will remain in place, but will add yet another layer to it. From the perspective of the care professional, manager and researcher, the recommendations would result in a new group of individuals who generally don't want to share their data but can consent to do so and a second group whose position remains as it is today, whose data can only be shared if they consent or if there is another legal basis. Whether these developments will contribute to greater professional and public understanding of their respective rights and responsibilities, is unclear.

Importantly there are no recommendations as to audit and traceability, as to enhancing transparency. The Review's starting point is that the public generally trust the NHS and trust the NHS with their data, though the available research suggests that the level of trust in the second case is half that in the first. The key to sustaining even that level of trust is transparency; nothing will undermine that trust more effectively than a sense of shadowy, public bodies having unauditable access to personal data. If an individual cannot find out who has their information and what use they are making of it, they cannot be '*absolutely clear ...when health and care information about them will be used'* as set out in the Review's terms of reference.

What is surprising is that there is no consideration of the precedents that are already operational. For example the Summary Care Record, where more than 50 million citizens have agreed to key data about their health and care to be stored by NHS Digital and to be accessed, subject to strict controls by authorised care professionals, with every instance of access, recorded and monitored. It is not clear why such a degree of monitoring and access control is appropriate for an individual's Summary Care Record but not considered for an their complete, confidential data set.

Despite the Review's conclusion that the majority of the population are in favour of their data being used for running the NHS and for research, there are no recommendations to make that sharing easier. Whilst a new opportunity for opting-out has been introduced there is no equivalent opportunity to register a general or defined consent, for example with respect to particular areas of research; no opportunity to opt-in.

What also remains unresolved is the future of the so-called Type 1 and Type 2 objections offered by the Care.Data programme, the issue which was largely responsible for the setting up of the Review in the first place. The Type 1 allows individuals to object to their data being shared by the GP with any organisation including NHS Digital and Type 2 giving them the right to object to NHS Digital disseminating their personal confidential data. The Review suggests that following consultation these objections '*should be replaced'*, although it is unclear how. Given the responsibilities of a GP as a 'data controller' under the Data Protection Act it seems unlikely that the right to make the Type 1 objection, restated by the Secretary of State in 2013, can be removed.

In its overall approach the Review takes a relatively narrow perspective, taking an NHS-centric approach. What is not considered is the revolution in the collection, control and use of personal data in the rest of the increasingly, digital world. In that world the direction is towards personal ownership and control of data in exchange for access based on shared risk and utility. Individuals may choose to share their data, sometimes foolishly, but they will have made a positive decision to do so. Whether the NHS cannot remain an isolated island in that increasingly digital world is open to question.

However given the unwillingness to invest sufficient political capital, the scarcity of expertise within the Department of Health and the developing crisis over NHS resources, there is little appetite for the root and branch reforms that are needed. As a result it is most unlikely that the 2016 Caldicott Review will be the last word on data privacy in health and social care. Perhaps its greatest impact will be to encourage ever greater numbers of individuals to take the only positive, proactive step open to them and to opt-out; a step that Care.Data encouraged more than 1.2million people to take in just a few weeks.