National Data Guardian for Health and Social Care's Review of Data Security, Consent and Opt-Outs

Response by the Wellcome Trust

6 September 2016

Key Points

- Public confidence is critical if the benefits of using health and care information are to be realised. This confidence can only be earned if the governance system underlying the proposed opt-out model is transparent, accountable and robust.
- Patients need to have clear choices about how their information can be used, and to know how these choices will be honoured. The NDG Review is a welcome step in setting out about what good governance should look like for patient information and must be the start of a conversation with the public.
- We broadly agree with the proposed opt-out model and strongly prefer a single opt-out question for patients.
- Without a realistic timetable for implementation past mistakes will be repeated. Considerable technical, policy and communications work will be needed to ensure that the proposed model can be properly and securely implemented.
- Clarity and honesty on what will happen to existing Type 1 objections are essential if patients are to have reason to trust that their choices will be respected.
- The newly formed independent patient data taskforce stands ready to work with the Department of Health on establishing the right model for supporting conversations about how patient information can be used.

About Wellcome

We are a major charitable funder of biomedical research in the UK, committed to improving health. The research that we support includes the Farr Institute and cohort studies, which collect and link biomedical, health and other types of data from large numbers of individuals over time to enhance our understanding of health and disease. We believe that the responsible use and sharing of data is vitally important for research and the development of evidence-based healthcare and services.

Our response focuses mainly on the opt-out model proposed by the NDG (**qs 11-15**). It also addresses broader issues of implementation and the governance framework necessary as we believe it is essential to get these right in order for the model to work in practice.

Alongside the Department of Health and several other funders, Wellcome is supporting a new independent taskforce[1] that will be working to improve conversations about data, developing a framework for clear discussions with the public, patients and healthcare professionals about how data can be used to improve health.

[1] https://wellcome.ac.uk/news/independent-patient-data-taskforce-announced

Proposed Data Security Standards

Question 4: The Review proposes ten data security standards relating to Leadership, People, Processes, and Technology. Please provide your views about these standards.

1. We welcome the proposed data security standards and consider them an important step towards improving the robustness of data governance right across the health and social care system. It will be important to ensure the right balance is struck between the safeguards afforded by the data security standards and the need to enable access to data to improve health and care. In implementing the data standards there is a risk that they will be perceived out of the broader context of the Review, focusing on tightening security without balancing this with the need to share when appropriate.

2. Implementing the standards will require significant resource both in terms of technical implementation and in terms of investment in people to help create a better data security culture within the health and social care system. Training, digital skills development and strong leadership are all required to ensure the standards can form the basis of best practice in data security.

Proposed Consent/Opt-out Model

Question 11: Do you have any comments or points of clarification about any of the eight elements of the model described above? If so please provide details in the space below, making it clear which of the elements you are referring to.

Terminology

3. **We caution against describing this model as a "consent/opt-out model".** Consent and opt-out are two very different models and it is misleading to imply that the model being proposed is based on consent. "Consent" implies there is active agreement by a participant to allow their data to be used and data will not be used without consent. "Opt-out" implies that participants have an opportunity to express an objection to their data being used. Without this objection, the data will be used by default. The model being proposed is an opt-out model.

4. The term "personal confidential data" has been in use since the second Caldicott Review (2013) and applies to data used by the HSCIC (now NHS Digital). The Information Governance Alliance share our concerns that term may be confusing to the public. We suggest that this phrase should not be used as the basis for the opt-out. Even though it is defined in a healthcare setting as information that is subject to the common law duty of confidence, the term "confidential" may mean different things to different people and in different contexts. For example, your name and address could be confidential if they are contained within a database of patients with a genetic condition, but not if they are part of the publically available electoral roll. Confidentiality refers to a relationship a person has to the data and the duty of care owed to that data, it is not a quality of the data itself. Patients will need real clarity in the opt-out model if they are to make a meaningful choice.

The opt-out model

Element 4: You have the right to opt-out

5. We support the adoption of an opt-out model for patients on the purposes for which their identifiable information could be used beyond direct care. An opt-out can provide patients with a meaningful choice, whilst ensuring that for those who do not object to their information being used, there is a default that maximises the research potential of this data. Robust epidemiological research relies on a high degree of coverage across the whole patient population. An opt-out model is more likely to deliver this than a consent-based model, which would be vulnerable to low or skewed response rates. An opt-out model is also less likely to result in bias in the sample that would undermine the validity of health research findings and put vulnerable groups at risk.

6. We strongly prefer a single opt-out question. While the option of two opt-outs appears to offer patients a greater degree of choice in how their information is used, in practice, care, service delivery, audit, service improvement and research cannot be distinguished easily into two separate categories. All of these activities exist along a continuum with the aim of improving health and healthcare. A two-option opt-out may also give the impression that the distinction between the options is between NHS and non-NHS uses: patients should not be given the false reassurance that they can limit information sharing to organisations within the 'NHS family'.

7. Many people's biggest concerns about data use centre on the issue of commercial access to data. Wellcome conducted extensive research on public attitudes about this issue and published a report earlier this year.[2] There are many commercial partners involved in data use right across the health and care system, including in the provision of direct care, and this should be acknowledged openly and transparently. The information provided to patients should be clear about the types of use and users of data so as to give them the best possible opportunity to understand the choice they are making. It is important to recognise that there could be commercial access in both categories of the two option opt-out.

8. People's baseline awareness of the fact that patient data may be used for purposes beyond care is generally very low, which means that a more complex opt-out might in fact confuse patients rather than empower them to make the choices that correctly reflect what they want. The choice being offered to patients is only meaningful if it is clear, accurate and easily understood.

9. The vast majority of uses of patient information would require only some specific data fields and thus a small proportion of the amount of data contained within a person's medical record. However, the phrase 'information' is used to cover everything from the use of a whole medical record (for direct care) right through to a small number of data fields (for other purposes). This increases confusion over what data is actually being used for what purposes and under what circumstances. It would help to inform the public and avoid misconceptions about what happens in practice if the opt-out model could make clear what is meant by 'information' in different contexts.

Element 5: This opt-out will be respected by all organisations that use health and social care information

[2] https://wellcome.ac.uk/press-release/public-need-know-how-patient-records-are-used-including-commercial-organisations

10. There are many types of data flow at both national and local levels, not all of which are registered centrally at the level of NHS Digital, for example, the agreement between the Royal Free NHS Trust and Google DeepMind that was reported in May 2016. If patients are to have confidence in the system, it is essential that an opt-out registered at their GP applies not only to national-level data flows managed by NHS Digital but to the myriad local and regional instances of data sharing such as this one. There needs to be a **clear articulation of how this can be uniformly implemented where data flows do not touch the NHS spine,** across individual health and care organisations, such as care homes and dentists, and local-level data sharing practices.

11. As part of this comprehensive system, an unambiguous statement on what does and what does not constitute 'direct care', applied across the whole system, would be extremely valuable, as much confusion and distrust arose over the Royal Free/DeepMind agreement's interpretation of 'direct care'. It should not be left to individual NHS Trusts to determine what this means in each case.

12. Additionally, there are many different opt-outs currently in operation across the system. If the proposed opt-out model is to provide a comprehensive framework that covers all identifiable data flows, it must be clear how these existing opt-outs will be managed. For example, the Summary Care Record (SCR), which allows GPs, pharmacists, A&E clinicians and some other healthcare providers to access basic patient information about medications and allergies, is currently subject to an opt-out, registered at the GP level. As the SCR is used for direct care, the wording of the Review (s.3.2.5-6) is not clear whether or not opt-outs for data flows such as the SCR would continue to apply in the new model.

Element 7: The opt-out will not apply to anonymised information

13. **We agree with the NDG proposal that the opt-out should apply only to 'personal confidential information'** (with the caveat about language noted in paragraph 4 above). However, this forms a small proportion of the data that is used and shared in practice across and beyond the health and social care system. There also needs to be clear communication about what happens to de-identified or anonymous data, how it can be used and how it is safeguarded. This would provide some valuable context to the model, particularly when engaging with patients about their choices over data use. Even if patients are not identifiable from the data, they may still have an interest in how it is used, for example, wanting it to be used only in the public interest and not sold to help companies better target their marketing, for example.

14. **Transparency on the rules** about the use and dissemination of de-identified data in addition to personal data would help ensure there are 'no surprises' about data use and is a necessary component for building public confidence about the system as a whole.

15. Much of the public concern about what happens to data arises because of confusion about what data can and cannot be disseminated for purposes beyond direct care. Use of the terms 'pseudonymised', 'anonymised' and 'de-identified' is muddled and it may not be clear to the public, or indeed data users, what data falls within scope of the Review model and what impact the new model will have on current practice. Removing identifiers from data and replacing with a code (i.e. pseudonymisation) does not constitute anonymisation of data.

16. The authoritative UK Anonymisation Network's Framework clarifies this distinction[3]. We commend the Framework to the Department of Health for a clear, comprehensive account of what needs to happen to data and the environment in which is it used in order for it to be considered 'anonymised' information. This a valuable resource alongside the ICO's Anonymisation Code of Practice for providing technical detail on anonymisation, but at the same time clear, unambiguous vocabulary in plain English is needed that is understandable to the general public. This is one of the foremost tasks of the independent taskforce on patient data. Getting these distinctions right will have a strong impact on the trustworthiness of the information governance system.

Question 12: Do you support the recommendation that the Government should introduce stronger sanctions, including criminal penalties in the case of deliberate or negligent re-identification, to protect an individual's anonymised data?

17. **We strongly support the NDG's call for criminal sanctions** to be available in cases of deliberate attempts to re-identify individuals using patient data. Sanctions can be an important part of the accountability that is required for a trustworthy system but they should be linked to the wider regulatory framework for data use, as patient data is not unique or isolated from other data types. With the Digital Economy Bill currently under Parliamentary scrutiny, it is timely for the Department of Health to consider how sanctions against patient data misuse should align with the broader governance framework for administrative and government-held personal data.

18. The wording of the conditions under which sanctions could be imposed needs to be clear to ensure that sanctions target the right kinds of behaviours without inadvertently penalising honest mistakes. We suggest that sanctions should apply in cases of unwarranted or malicious attempts at re-identification.

19. Sanctions should be proportionate to the nature and scale of the breach. Different types of sanctions will be appropriate depending on whether it is an individual or institution at fault, for example, or whether individuals suffer harm as a result of the data misuse. Clarity on the types of sanctions the NDG supports would be welcome.

20. Sanctions can function as an effective deterrent against misuse and help promote good practice if they sit within a broader governance system that is clear to all stakeholders, with transparent decision-making and effective monitoring or auditing. Implementation of the proposed model should take this into account with sanctions developed as part of this wider governance framework.

Question 15: What are your views about what needs to be done to move from the current opt-out system to a new consent/opt-out model?

Existing opt-outs and future proofing

21. The Review recommends that the 'status quo' be maintained until a full consultation and further testing is carried out on the proposed opt-out model. We agree that historical Type 1 objections need to be honoured, to ensure patients have reason to trust that their wishes are being respected and to build confidence in the system. It is imperative

[3] The Anonymisation decision-making framework. M Elliot, E. Mackey, K. O'Hara & C. Tudor (2016) UK Anonymisation Network (p.16) http://ukanon.net/wp-content/uploads/2015/05/The-Anonymisation-Decision-making-Framework.pdf

that during this time careful consideration is given to how any changes to their validity under the new model will be managed, both for patients and for GPs.

22. We recommend that the NDG is involved in the final decision the Department of Health makes about existing objections. Formal approval from the NDG will provide clear accountability, bolstering public confidence that decisions about patient information are being made openly and are subject to independent scrutiny.

23. Where an individual has registered a Type 1 objection, they have expressed a clear choice for their information not to flow beyond their GP. They are therefore more likely than the general public to be concerned about what happens to their information and their concerns must be addressed. We recommend that existing Type 1 objections be honoured but if this choice is no longer going to be available as the new model is implemented, these patients should be contacted directly by their GP with a clear explanation of what has changed, why, and what their options are in light of the new model.

24. It is essential that the Department of Health works with GPs and takes concerns about their duty of care towards their patients seriously. It was evident during the initial launch of *care.data* that many GPs were deeply unhappy about the proposals and some took the step of opting out their entire practice list. It will be extremely important to have considered discussions with GPs about how they can balance their responsibilities as data controllers with the obligation placed upon them to allow personal information flows to NHS Digital. Otherwise, it is likely that the proposed model will face another backlash from the primary care community. GPs are also the key gatekeepers for informing patients about how their information is used and their support will be indispensable if patients are to have confidence in the model.

25. Advances in technology and data processing capacity mean that there are likely to be substantial innovations in the way that data can be accessed, used and linked over the coming years, which may lead to exciting developments for health care and research. There is a risk that the model will quickly become obsolete if it is tied too closely to existing NHS processes and practices. The opt-out should be able to accommodate changes to these over time without risking public confidence in how the system is managed if there is transparency and public accountability over how decisions are made, for example about when and how patient datasets could be used in machine learning to create new diagnostic algorithms.

Implementation

26. It is vitally important that there is an **appropriate timescale** for fully developing, introducing and implementing the opt-out model. While there is an urgent need to improve the consistency and quality of data flows to enable better research and improve healthcare delivery, rushing the process will inevitably result in a repeat of past mistakes and the opportunity to build public buy-in for health data use will, we believe, be lost completely. We urge the Department of Health to take sufficient time to get this model right: there is a great deal of careful work that needs to be done on technical implementation, ensuring appropriate governance is in place and on communicating the changes to patients across the country in a way that is clear, accurate and allows them to easily and meaningfully express a choice.

27. **Technical implementation** of the opt-out right across the health and social care system will be a substantial challenge. Even if the opt-out is registered on the NHS spine, there are nearly 30,000 health and care organisations that are not spine-connected[4]. We are therefore unsure how the promise to uphold opt-outs across the system can technically be upheld given the constraints of the current information system architecture. Just as importantly, a shift in culture towards secure, consistent, comprehensive implementation of the opt-outs across the system will need to be embedded to ensure that they are actually upheld in practice.

28. The **practical implementation** of the model also needs to be taken into account: at present, the vast majority of people do not have active online access to their GP records and the model will need to work as a paper-based system as well as an online one in the interim period before online access is the default for patients.

Communication

29. **We support the single opt-out 'information profile'** approach to the opt-out and consider it to be clearer and easier to understand than the tick box approach. The 'profile' makes it clear to individuals that there is a default setting and they can select an alternative option. However, the distinction between the 'limited' and 'restricted' settings on the two opt-out information profile model is very unclear. The alternative requirement to tick a box to express *not* agreeing with the conditions of sharing seems more likely to create confusion among patients.

30. It should not be implied that health data will never be used for insurance purposes as it is a standard part of applications for some forms of insurance that insurers seek to gain access to parts of an applicant's medical records via their GP, with the individual's permission for that specific instance of data sharing.

31. Getting communications to patients and the broader public right will be critical to build public confidence and ensure the success of the model. It should be recognised that local or regional communications may be more effective than a national-level strategies in some instances. There is much to learn from local initiatives, for example from the implementation of innovative health records management systems such as the Leeds Care Record.

32. GPs are the data controllers for patient information. They have a duty of confidentiality towards their patients and will often be the front line source of information on the opt-out for them. If, as the Review model proposes, GPs will be unable to prevent data flowing from their practices to NHS Digital, we urge the Department to **engage fully with GPs** at the earliest opportunity to discuss the rationale for this approach, listen to their concerns and work collaboratively to build their support.

33. The newly-established taskforce will include work on how to get the language about data right to ensure people can receive meaningful, honest information about their choices. We look forward to supporting the taskforce as it engages with the Department of Health on the development of communications about the opt-out model, to ensure that this vital part of the implementation is done well.

[4] Data from presentation given by Prof Martin Severs (HSCIC) to Research Advisory Group, June 2016

34. The NDG Review creates an opportunity to learn from past mistakes, fix the governance system and develop a clear framework for patient information that people are able to support now and in the future. But the Review also leaves many questions unanswered and getting the implementation of the model right will be crucial. Recent critical media coverage about the reintroduction of *care.data* suggests that there is a very real risk of further failure and loss of public trust. This would have a devastating impact on research, on healthcare delivery and ultimately on patients. The new opt-out model is too important to get wrong.