September 2016

Response submitted by:
Sobia Raza
sobia.raza@phgfoundation .org
Alison Hall
alison.hall@phgfoundation.org

National Data Guardian for Health and Care's review of data security, consent and opt-outs: response from the PHG Foundation

This review by the National Data Guardian for Health and Care (NDG), Dame Fiona Caldicott, makes recommendations to the Secretary of State for Health. These are aimed at strengthening the safeguards for keeping health and care information secure and ensuring the public can make informed choices about how their data is used.

The NDG proposes new data security standards for the NHS and social care, a method for testing compliance against the standards, and a new opt-out to make clear how people's health and care information will be used and in what circumstances they can opt out. Below is the *verbatim* response from PHG Foundation to the main questions in the related consultation.

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

This response applies to all ten proposed data security standards.

Collectively the proposals on strengthening safeguards for data security are timely and proportionate, striking a balance between ensuring security and not hindering the delivery and development of care. Enacting the recommendations on safeguards will be a vital step in reassuring patients that the NHS is competent at handling their data, as well as ensuring that the NHS's digital infrastructure and technologies are up-to-date and fit for purpose.

Mandating these requirements both through this Review and the associated CQC recommendations will help Trusts and CCGs to prioritise policy development and investment in these areas. In doing so, involving other regulators such as the CQC and the ICO in the development of coherent approaches will be vital in order to avoid inconsistency and wasteful duplication of effort.

Question 6: by reference to each of the proposed standards, please can you identify any specific or general barriers to implementation of the proposed standards?

This response applies to Data Security Standard 1. All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes.

And to Data Security Standard 8. No unsupported operating systems, software or internet browsers are used within the IT estate.

Replacing obsolete technology (Standard 8), and ensuring that staff are adequately equipped to handle personal confidential data appropriately (Standard 1) will ultimately require fundamental improvements in digital and data infrastructure. Even with the best intentions, staff will not be in a position to deliver on Standard 1 unless they are provided with appropriate tools which both enable and empower them to handle data appropriately. For example, our engagement with the clinical genetics community has identified the need for a single, central, secure NHS database of genomic variants, particularly as rare genomics variants may in some circumstances constitute personal identifiable data. In the absence of such a resource, the sharing of genomic variant data -which has important implications for patient safety and service quality – cannot and does not currently take place at optimal levels. In other work evaluating the potential for novel technologies to be utilised within

the NHS (*Realising Genomics in Clinical Practice*) or public health (*Pathogen Genomics into Practice*) it is clear that some types of data such as genome sequence data will place additional demands on people and healthcare infrastructures which will require dedicated investment above and beyond that being committed to research projects such as the 100,000 Genomes Project.

It will be vital to review whether the current NHS digital investment plans can deliver the dedicated resources required to realise Standards1 and 8. In relation to Data Security Standard 1, more explanation is needed of what constitutes 'appropriate' purposes. This term seems somewhat subjective and it is unclear how the requirement for appropriateness relates to the additional requirement for 'fair' processing as enshrined in schedule 1 of the Data Protection Act 1998.

Question 7: Please describe any particular challenges that organisations which provide social care or other services might face in implementing the ten standards.

In order to deliver prompt, efficient and effective care to individual patients, health and social care services need to exchange information including patient's personal confidential data. Ensuring safe, secure and prompt data sharing is likely to be challenging when personal data is transferred between people who have different entitlements according to their role based access requirements across health and social care.

Question 10: do you agree with the approaches to objective assurance that we have outlined in paragraphs 2.8 and 2.9 of this document?

In principle, we support the approach outlined in paragraphs 2.8 and 2.9 i.e. to have an objective standard and then measure performance against this, with that assessment being done by appropriately qualified assessors. However, there is a lack of clarity about many of the elements that have been identified, and their acceptability will depend very much on the scale of what is being proposed and how it is implemented. Outstanding questions include:

» What the 'redesigned IG toolkit' will look like

» Whether it will be reasonable, proportionate, feasible, and comprehensible

» The extent to which there will be a process of engagement and consultation to update it or whether it will it be imposed from above

» The nature of the sanctions for being designated as being an 'at risk organisation'

» The support (in terms of advice; guidance; training; education and support) which will be available to those users who are struggling to comply with the re-designated IG standards and the costs imposed

The claim that CQC will use this to 'prioritise' action seems valid but it is unclear whether this involves more frequent, comprehensive inspections and possible penalties. These should be proportionate to the risks associated with continuing bad practice.

Whilst peer support can be a valuable tool to encourage and sustain behaviour change in other contexts, it is important that sufficient additional resources are made available for guidance, mentoring etc. to underperforming organisations. What incentives will be put in place for the better performing organisations and individuals to be involved?

Question 11: Do you have any comments or points of clarification about any of the eight elements of the model described above?

We strongly support the office of the National Data Guardian and welcome the fact that this role will shortly be enshrined in statute. Health and social care providers require access to potentially sensitive information about patients and their families in order to deliver safe, effective services, and it is right that data processers and controllers should take this duty seriously. Therefore we strongly endorse Recommendation 10 of the consent / opt-out which states that the case for data sharing still needs to be made to the public, and that all health, social care, research and public organisations should share responsibility for making that case. PHG Foundation is taking this responsibility seriously and is actively engaged in work that highlights the potential benefits, burdens and risks associated with data sharing.

We also welcome the publication of this Review and support the fundamental intention of this exercise to address the question of '*what more can be done to build trust in how the NHS and social care services look after people's confidential data and use it appropriately*' [Section 1.1. of the Review]. Yet in assessing this question the Review was specifically directed from the outset to consider '*a new consent or opt-out model for data sharing*' as a key approach for building and re-establishing trust. We therefore feel that this Review has not had the opportunity to undertake a balanced and warranted assessment of the merits and drawbacks of alternative approaches to nurturing trust and to harnessing data for the benefit of patients. In this regard our concerns with the eight point model as a whole are as follows:

The provision of an opt-out model will not necessarily increase public trust

Whilst we acknowledge the importance of fostering public trust in health data sharing, we have significant concerns with the consent/ opt-out model as a whole. The implicit assumption of the model is that providing individuals with more detailed control about the use of their personal confidential data will enhance individual autonomy, promote empowerment and ultimately improve trust in systems and their trustworthiness. The report does not attempt to challenge this

assumption or reflect on the effectiveness of the model against alternative approaches. We think that offering individuals the option to 'opt-out' of health data sharing will at best only offer a stop-gap solution to address the lack of trust and public's concern, and at worst risk a repeat of the care.data experience. Focusing on a mechanism for opt-out rather than addressing more specific concerns will further postpone a transparent discussion with the public about their expectations of a future health system and the role health data will play in it. Indeed, instead of improving trust offering 'opt-outs' could compound people's concerns about data and actually reinforce the perception that any trust in NHS data handling is unjustified. Rather than focussing on building trust through offering opt-outs, we believe that efforts should be re-focussed on holding a more transparent debate about what is required, as part of the social contract, to build personalised and innovative healthcare for all citizens, and the role of health data in building a sustainable health system now and for future generations.

The model fails to address the most pressing public concerns

Empirical studies have consistently demonstrated that the public distrust use of their data for marketing or insurance purposes. Point 1 of the model alludes to this concern. However, the only way that an individual can prevent their data being used in this way is to opt-out of their personal confidential data being used for any purpose other than direct care. Limiting the scope of the opt-out in this way has serious potential consequences. Moreover given the opt-outs will not apply to anonymised information, it's unclear whether anonymising data will be enough to assuage public concerns around sharing data with commercial organisations.

Implementing the proposed consent / opt-out model could have serious consequences for medical research

Some types of medical research rely on accumulating information about large numbers of people. This is the case with genetic epidemiology research which aggregates health data from thousands of people to determine whether a particular genetic / genomic variant is associated with disease. When variants occur infrequently in a population the numbers required to establish statistical significance become correspondingly higher. However, certain genetic / genomic variants might be very rare, and therefore potentially more identifying than other types of genetic / genomic variants when combined with other data as there is a gradation of potential for identification depending on their type and nature. In some circumstances, this might also involve the use of additional personal confidential information since this is necessary to understand the nature and complexity of a person's condition. With such high numbers involved, gaining consent from each potential participant for this type of research would not be feasible (on grounds of practicality

and expense). Thus if the proposed consent / opt-out model were to be implemented in its current form – such research could not continue. This would have profoundly detrimental implications for patients and families affected by rare genetic diseases.

Empowering patients to make informed and autonomous choices

As an organisation committed to personalised healthcare, we strongly support a more open and transparent health service, where patients are empowered to make more informed choices about their care. But we also believe that patients need to understand that their personal confidential information is crucial in creating a learning healthcare environment where delivery of safe, high quality, evidence based care is paramount. Enabling patients to appreciate the value of their health data in building better care within the NHS requires a new relationship between patients and the health service.

The limitations of anonymisation

Element 7 of the consent / opt-out model confirms that '*the opt-out will not apply to anonymised information*'. This seems to be predicated on the assumption that the anonymisation processes can always prevent the identification of individuals from their linked health data. In fact, the extent to which health data can be effectively anonymised depends very heavily on context. For example, it is more difficult and perhaps impossible to effectively anonymise cases which involve very rare genomic variants in small numbers of people inherited within families. Anonymisation therefore has limited applicability and utility when applied to genetic / genomic information. As an organisation we have examined the challenges of anonymising genomic data in detail, however the limits to anonymisation extend to linked health data more generally. We discuss these challenges below.

Anonymisation and genomic data

Genomic data are difficult to render anonymous while also using them productively – they can be strongly identifying and the uses to which they are put can be undermined if data are manipulated in certain ways. However anonymisation techniques are very important in genetics and genomics because alternative legal grounds for lawful processing such as obtaining consent are often restricted for practical and logistical reasons (due to the numbers of people involved). Since the effectiveness of de-identification depends heavily on the nature of the data and the context within which such data is used, and the network of associations made with other datasets (and genetic / genomic data may be linked with many and diverse data) – the process of anonymising genomic data is often challenging. This is compounded by the fact that the current EU data protection regime protects personal data, offering little to no protection in respect of data that cannot be used to identify a person.

Anonymisation and linked health data

The trade-off between rendering data anonymous whilst maintaining its utility also applies to health data more generally. Whilst data-points in isolation might be considered anonymised, their combination and linkage to other datasets exposes them re-identification, yet it is exactly such linkage of different health data which determines its utility. Looking forward, the limitations of anonymisation are likely to apply to other 'omics data types as well as other complex-health data which are often highly personal to the individual from whom they are derived, (e.g. microbe, telehealth / remote monitoring, imaging data). Moreover in an information-rich era and that of 'big data' analytics, anonymisation of even the more 'conventional' health data types will be increasingly challenging to achieve.

There is lack of reference within the Review as to what will constitute anonymised data. Since the ability to effectively anonymise data - particularly linked health data - depends on context, the risk and probability of re-identification occurring and the harms under these circumstances should be considered in order to inform a proportionate approach. If linked health data were to be shared on the basis that is 'anonymised' but instances of re-identification emerge this will serve to undermine public trust. At the same time if the extent of data shared is strictly constrained this will severely impact the delivery of services and medical research which relied upon this data. To reiterate, rather than offering opt-outs on personal confidential information or sharing linked-health data on the basis that it is anonymised, we believe that a transparent debate with the public should be supplemented by discussions about the limits of anonymisation and the alternatives.

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

We strongly support the recommendation that the Government should introduce stronger sanctions, including criminal penalties in the case of deliberate **unlawful** re-identification. This follows recommendations in a report from the Nuffield Council on Bioethics *Biological and health data: ethical issues*, that criminal penalties, including imprisonment [comparable to those applicable offences under the Computer Misuse Act 1990], be introduced for the deliberate misuse of data, whether or not it results in demonstrable harm to individuals. However, extending the criminal offence to instances of negligent re-identification has less justification and requires careful analysis. In general, criminal penalties such as imprisonment are not applicable to tortious offences such as negligence.

Creating more effective sanctions for deliberate re-identification is consistent with increasing use of contractual undertakings not to seek to re-identify individuals without due cause in data sharing agreements between health care providers and secondary data users and also in employment and honorary contracts within health and social care. Provision for criminal sanctions would have the advantage of having a deterrent effect and also in highlighting the potential seriousness of the offence. However it is important that sufficient resources are available to police any sanctions that are introduced, and also that the penalties have the backing of the judicial system. There have been examples in other statutes, (such as the Human Tissue Act 2004) where criminal sanctions have been introduced but a minimal number of prosecutions have been brought.

Question 13: if you are working within health or social care, what support might your organisation require to implement this model, if applicable?

The fact that the model consent / opt-out is intended to operate as a single choice which will be implemented across all settings implies that there will need to be an infrastructure for sharing details of patients and the public who have chosen to opt-in or out of the system. This needs to be robust and secure and accurate. The Review does not make it clear how such a system will operate, and how individuals may register their preferences, and whether this needs to be done through a health or social care provider.

Question 14: if you are a patient or service user, where would you look for advice before making a choice?

Patients have traditionally sought advice from their GP (for example in relation to the creation and opt-out of summary care records). This is why organisations such as the British Medical Association potentially have an important role to play in mediating the relationship between their members (who are medical practitioners and general practitioners) and the public, and in influencing the materials that are made available to patients through public education and engagement. More recent experience of the care.data roll out demonstrates how important this role might be with some practices registering up to 100% of their patients for or against opt-out. Other organisations such as Royal Colleges also have a role to play in producing relevant professional guidance.

In the context of rare diseases, patient associations and umbrella groups such as Genetic Alliance and Unique could be influential in providing a source of independent advice. Other possible sources include the NHS Constitution and supporting documentation (although it's not clear how widely this is used by patients).

If the model consent / opt-out is implemented in its current form, it is vital that it is supported by a concerted attempt from all health providers and other stakeholders to illustrate the importance of this choice and its potential implications. This should be done through a variety of means including social media, websites but also by letters and posters to ensure that those who do not have access to the internet or computers are not disenfranchised through lack of information. Moreover, in order to enable individuals to make the most informed choice regarding their consent / opt-out preferences, a significant concerted effort at public engagement should precede the implementation of the model. This is especially vital given that the Review has found that current public understanding of the use and benefits of information sharing is limited.

Question 15: what are your views about how the transition from the existing objection regime to the new model can be achieved?

Please comment on your answer

It is clear that the existing regime is dysfunctional in a number of ways:

» There is a bewildering array of different opt-outs available to patients

» Those that do exist (such as objections which restrict the secondary use of data from primary care (Type 1 objections) and the ongoing use of data for secondary purposes by the HSCIC (Type 2 objections)) are limited either in their scope or in the extent to which they have been implemented

» These organisational failures (such as the HSCIC's failure to implement systems to enable Type 2 objections to be logged) have received a lot of negative media attention

» In addition to the challenges with the objection region, the current arrangements for following and applying information governance guidance have resulted in inconsistencies in information-sharing practices across organisations and between NHS Trusts.

As a result of these factors, there is such a profound lack of trust in the processes and leadership of existing organisations that this situation is difficult to rectify.

The solution, in our view, is not to seek to build public trust by extending the scope of opt-outs to encompass all purposes beyond direct care. This is because implementing the proposed consent / opt-out model does not address past institutional failures or enable processes and organisations to be built that are based on trustworthiness and proportionality.

Our view is that - following on from empirical work such as the IPSOS Mori and Wellcome Trust report *The One Way Mirror: public attitudes to commercial access to data* - that public engagement and education programmes need to be built around demonstrating why sharing personal confidential data is key to safe and effective healthcare and that the people involved are trustworthy rather than focussing only on the technical aspects of the data sharing or the infrastructure and processes that will be used. Monitoring the consistency with which processes and guidance are implemented across the health system will also be vital to fostering trust by minimising variation in practice and its impact on the quality of healthcare services provided.

Question 16: do you think any of the proposals set out in this consultation document could have equality impacts for affected persons who share a protected characteristic, as described above?

In the context of genetic and genomic medicine the proposals for a consent / opt-out model could have significant negative impact on two sets of users with protected characteristics under the Equality Act 2010 - ethnic minorities (race) and persons with disabilities. The reasons for this are as follows: Rare diseases are a significant cause of disability in the UK. At least 80% of rare diseases have an underlying genetic origin and so genetic testing is integral to the diagnosis of many rare diseases. Genetic and genomic testing services rely on being able to access and share genetic, genomic, and supporting clinical data in order to deliver safe and effective care to (rare disease) patients. This is because determining the genetic basis of a patient's rare disease relies on access to existing knowledge and data on both patients with the same or similar disorder but also data from the wider population. In fact, lack of consolidation of comparison population genomes can lead to potentially damaging misdiagnosis. Moreover, an individual's genetic data is best assessed in the context of wider data from an ethnically matched population. Under-representation of different ethnic populations in genomics databases can result in these groups being disproportionately likely to receive an incorrect genetic diagnosis for a disease.

In short ineffective data sharing results in delays to diagnoses, misdiagnoses, and inequalities in access to testing. The introduction of opt-outs on data sharing could therefore jeopardise existing practices and the future improvement of genetic and genomics services, with particular implications for the safety and quality of services for rare disease patients as well as ethnic minorities with rare diseases where there is insufficient representation of these groups in shared datasets. The rare nature of these diseases means that even a few opt-outs could undermine the ability to accurately diagnose patients, particularly where the analysis of their genome requires a 'match' with a patient with similar condition. Looking further ahead as the contribution of genomic effects to common complex diseases (cancers, heart disease etc) becomes more widely understood, the opt-outs could have a wider effect on population healthcare.

Question 17: do you have any views on the proposals in relation to the Secretary of State for Health's duty in relation to reducing health inequalities? If so, please tell us about them.

See response to Question 16 above.

The NHS ambition to utilise technology and data to improve health and health and social care delivery is central to the *Personalised Health and Care 2020 Framework* and *Five Year Forward View*. These reports note the key role for technology and data in helping to tackle inequalities and the risks of causing health inequalities to widen if we fail to '*get serious about prevention*'. The use of health data is integral to this agenda. It is crucial to acknowledge that the development and delivery of personalised care and personalised disease prevention that can meet the needs of a diverse population hinges on the availability of health data which reflects population diversity. For the reasons outlined in our responses to Question 11 and 16, the proposals on opt-outs as set out in this Review could undermine the ability to obtain datasets that are fully representative. As a result, this could:

(i) Potentially increase health inequalities for subsets of the population who might be under-represented in datasets -including vulnerable persons and persons with protected characteristics; and

(ii) Undermine the development of personalised medicine and in particular, personalised prevention, due to lack of information on a wider population set.

More effective targeting of prevention, diagnosis and treatment through personalisation, and building better healthcare for the future rely on acting now to develop effective and secure data sharing.