THE FARR INSTITUTE RESPONSE TO THE NATIONAL DATA GUARDIAN REVIEW OF DATA SECURITY, CONSENT AND OPT-OUTS

This document is a response on behalf of the Farr Institute to the June 2016 Review produced by Dame Fiona Caldicott at the behest of the Secretary of State for Health. We offer comments on the Review by Recommendations, linked where appropriate to particular paragraphs. The Farr Institute very much welcomes the Review that, in many ways, reflects the ethos and the objectives of the Institute itself.

The Farr Institute is a UK-wide research collaboration involving 21 academic institutions and health partners in England, Scotland and Wales. Publically funded by a consortium of ten organisations led by the Medical Research Council, the Institute is committed to delivering high-quality, cutting-edge research using 'big data' to advance the health and care of patients and the public.

The Farr Institute does not own or control data but analyses data to better understand the health of patients and populations.

The Farr Institute operates across six broad themes of work:

Research: performing pioneering interdisciplinary research with large and complex data.

Skills: developing skills, talent and expertise in the health informatics research community and providing tools for collaborative working.

Public Engagement: engaging with the public to demonstrate the benefits of using health data in research and to encourage the support of secure and trusted access to patient information.

Methods: enabling new datasets and developing new infrastructure, methods, and technologies, and standards for new health informatics research.

Creating Partnerships: bringing together government, public sector, academia and industry to foster relationships and establish best practices for innovation and discovery.

Regulation and Ethics: working with the owners and controllers of data to support the safe use of patient information for medical research across the UK, championing data protection, confidentiality and privacy.

RESPONSE

Foreword

In her Foreword, Dame Fiona emphasises the crucial importance of demonstrating trustworthiness in the use of personal confidential information. We believe this is precisely the challenge that frames everything that must be done to deliver on the Recommendations arising from this Review. The challenge itself must, however, be appropriately set. We would contrast this early tone with the first paragraph of the Review that talks about 'building trust'. It is not possible to build trust. No actors in this field – be they regulators, data controllers, data owners, or researchers – can *build* trust. Trust is not something that can be constructed. Only citizens can give or take away their own trust. They are more likely to give trust to institutions and individuals that demonstrate that they are trustworthy, but even this will not necessarily ensure that trust is forthcoming. This is not just a question of semantics. It matters very much that everyone understands where the balance of control lies – it is with the citizen.

In the spirit of the trustworthiness theme, we were heartened by the obvious commitment to security and protection that was clear in the report. However, we detected a series of misunderstandings relating to scope and relationship between a series of information and cyber security standards and pseudo-standards that the report refers to. We attempt to comment upon this and suggest ways to ensure that available guidance is used to help clarify rather than hinder effective understanding and guidance that the proposals are attempting to offer.

The review clearly relates to England, but it would be useful to include a straightforward statement about the status of the review across the UK. Personal confidential data are to be passed to the HSCIC (NHS Digital) but it's not clear about other parts of the UK.

Recommendation 1

The leadership of every organisation should demonstrate clear ownership and responsibility for data security, just as it does for clinical and financial management and accountability.

Leadership is indeed crucial to success in this area. But different organisations are at different stages of preparedness for sharing, especially if a wider remit is envisioned to include data access for research and other secondary uses. We believe that there are three important respects in which leaders can be better supported.

1) Assessing preparedness for data use

Our work with our sister collaboration, the ESRC Administrative Data Research Network (ADRC), has developed a decision-making template to assist leaders and other decision-makers within an organisation to assess their preparedness for data sharing, and to help diagnose on-going challenges or barriers to effective data use. Our template is based on research that shows that – from an institutional cultural perspective – a culture of caution can have many compounding causes. The Review acknowledges a culture of risk aversion at 2.4.4. and says that 'Leaders should address cultural barriers by proactively engaging staff and involving national workforce organisations to support professional capability in this area.' But how?

It is commonly stated issue that the complexity of law and regulation is a barrier to sharing. The Review itself alludes to this in 3.2.22. Our research suggests, however, that the law itself is rarely the main issue in play. And if leaders do not have means to enquiry of their institution what is happening to drive the culture, then any attempt at change can be misdirected and ultimately thwarted. Our decision-making template assists in this regard by helping to reveal dynamics in play. We suggest this could be a useful tool in giving effect to Recommendation 1.

More information is available here:
https://www.youtube.com/watch?v=9H1wpoAwmZc

2) Support data controllers

Our work with the Scottish Health Informatics Programme (2009-2013) was a forerunner to our current work within the Farr Institute. Our research during that initiative revealed a great deal of anxiety among researchers and their host institutions about when and how the status of Data Controller was acquired (or lost). We developed brief guidance on this point, which might still be useful and/or adaptable to the current context.

Guidance on Data Controller status: http://www.scot-ship.ac.uk/sites/default/files/Reports/Appendix_6.pdf

3) Regulatory Stewardship

We believe that it is vital to success to put in place the appropriate mechanisms that will support a culture of confidence in responsible and safe data use. The Review makes many helpful points in this regard. To this we would add a further consideration, which we term regulatory stewardship. This refers to the crucial role played by many actors within the information governance landscape who serve to guide researchers and other through the difficult terrain. Informally, this kind of role can be played by Data Protection Officers or R&D Managers. Too often, however, the role is invisible and informal. One of the key recommendations arising from our work on SHIP was the recommendation for organisations to create Research Coordinators to perform this function. There are, of course, significant resource implications to be considered. Nonetheless, we suggest this is a role of crucial importance to be acknowledged and supported by leaders.

Further discussion of Research Coordinators can be found at para 6.6.2 here:
http://www.scot-ship.ac.uk/sites/default/files/Reports/SHIP_BLUEPRINT_DOCUMENT_final_100712.pdf

Recommendation 2

Recommendation 2: A redesigned IG Toolkit should embed the new standards, identify exemplar organisations to enable peer support and cascade lessons learned. Leaders should use the IG Toolkit to engage staff and build professional capability, with support from national workforce organisations and professional bodies.

We entirely endorse the need to enable peer support and facilitate cascade learning. The Farr Institute is developing 100 national case studies that showcases not only the work of The Farr Institute but of the wider UK research community. By publishing these case studies, the Institute aims to promote the safe and trusted use of data in research and raise awareness of its benefits to patients and the public. This also reflects the call elsewhere in the Review that the case for responsible data use must continue to be made to the public: **Recommendation 10**.

More information is available here: http://www.farrinstitute.org/public-engagement-involvement/100-ways

In paras 2.2.1-2.2.2 the point is made – and well taken – that sometimes there can be too many pieces of guidance in the development of standards. We endorse an infrastructure that is oriented towards leadership by examples. The SHIP Blueprint embodies a good governance framework that is based on Principles and Best Practices. The underlying idea is to support responsible data use while acknowledging that there might be a range of ways to act responsibly. Focussing on best practices provides illustrative ways through the regulatory maze.

We are concerned that the Review might send mixed messages at some points. There is a clear message running throughout that good governance is a collective responsibility, but at some junctures the focus seems very liability-oriented at the individual, personal level. Consider, for example, Data Security Standards 2 and 4:

Data Security Standard 2. All staff understand their responsibilities under the National Data Guardian's Data Security Standards including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.

Data Security Standard 4. Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.

Our commissioned work for the Nuffield Council on Bioethics into harms arising from data misuse confirms the view offered in the Review that most data breaches arise from maladministration rather than malevolence. This, then, is a systems issue more than anything else. While to Review points to the lessons from the airline industry, the re-enforcement of personal liability through various standards or recommendations might hinder the move towards the culture of learning that is recommended. How can institutions be better supported in this transition? Our research suggested that '…there are, broadly, three types of 'offender'. The first is incorrigible; there is little likelihood of correcting such behaviour and future intentions. Here, harsh sanctions are necessary up to and including dismissal. The second offender type has acted intentionally, but attitude and behaviour change is possible. The third is the unintentional offender. **Key recommendations:** For types two and three offenders, the action must be considered in context. It is crucial that these individuals can speak without fear about their motivations, which must be established clearly in order to put the best and most appropriate corrective measure in place. Corrective measures should aim to foster conformity (attitude and behaviour changes) and not compliance (only behaviour changes, the attitude regarding abuse/misuse of data remains). Re-training measures should reflect real-life situations, such as group work with patient stories.' Additional and more severe sanctions have their place, but if applied inappropriately, they may hinder data sharing without adding safeguards.

See further: A Review of Evidence Relating to Harm Resulting from Uses of Health and Biomedical Data (2015), available at: http://nuffieldbioethics.org/wp-content/uploads/A-Review-of-Evidence-Relating-to-Harms-Resulting-from-Uses-of-Health-and-Biomedical-Data-FINAL.pdf

Thus, we endorse Recommendation 9 (below), while suggesting that the full picture requires a diverse course of action to set the tone for the cultural shift that needs to occur.

We note that Recommendations 3 – 8 focus in more detail on the specifics of information security. We had a number of concerns generally about the wording and understanding of information security management that we were able to glean.

Whilst we entirely support the development of leadership obligations and their use to define a series of data security standards, we must point out that these standards are actually directives. As the report rightly points out, there are already a plethora of standards that is causing confusion across the health data management community. Developing a further set of standards seems unhelpful, particularly when the wording of these data standards is far more directive; their description should not misrepresent that.

There is an apparent misunderstanding within the report about the role of specific standards and toolkits, which is demonstrated by the example of Case Study 4. For instance, organisations are certified ISO 27001 compliant, not accredited. People are accredited – so a professional can be accredited as an ISO auditor, for example, who will then be able to assess an organisation's compliance with ISO 27001, and independently certify it if it satisfies the audit requirements.

The Cyber Essentials package is a subset of what ISO 27001 covers, so should not be represented here as an alternative to ISO 27001 – in effect, the case study is comparing apples to the crate that they are stored in.

As a series of standards, ISO 27000 attempts to comprehensively guide organisations in information security management. ISO 27001 is a standard that defines information security management requirements and is needed to establish the basis upon which a management system will proceed. ISO 27002 helps organisations specify a code of practice to implement those requirements. The 2005 version of 27002 was in part the basis upon which the IG Toolkit was originally developed. However, perhaps some of the confusion and issues with the IGT have resulted from the divergence or in some cases little or no regard for the requirements established in ISO 27001 – you cannot successfully implement 27002 without regard for 27001, partly because 27001 shows that an organisation and critically its people understand the requirements.

What is clear is that there remains a lack of understanding about the core security fundamentals and the emergence of a "cherry picking" approach to security standardisation and implementation of protection approaches where they are deemed to be affordable and practicable. This strategy does seem piecemeal and does not demonstrate the understanding of risk, mitigation strategies, management commitment and amongst other things policy development that help specific organisations to implement tools such as a Cyber Security Essentials package.

This should not be taken to mean that we mandate ISO 27001 certification for organisations across the NHS and its data sharing partners (for interest we refer you to a publication that the Farr collaborators authored that describes some issues and implementations in more detail, and their relationships to trustworthiness: http://medinform.jmir.org/2016/2/e22/ . We would however point out that in terms of cost and affordability, the British Standards Institute permits some access to ISO standards, including the 27000 series, by virtue of having been licensed to some academic and public sector organisations. It would be worth organisations checking whether they have access at no extra cost, and seeing the extent to which they may be able to implement some of the foundational elements that 27001 provides.

With this in mind, we will reply to each of the following recommendations 3 – 8 and highlight where this may be causing issues.

Recommendation 3

Trusts and CCGs should use an appropriate tool to identify vulnerabilities such as dormant accounts, default passwords and multiple logins from the same account. These tools could be also used by the IT companies that provide IT systems to GPs and social care providers.

A risk with this approach is that the tool will not be able to identify all dormant accounts, default passwords and multiple logins, whilst a routine check on these aspects can be made policy and enacted as part of a management process. Login locations can be defined as part of the management monitoring for systems, and whilst the examples above are "rookie mistakes" for systems security management, it is incumbent upon an organisation to be able to identify other risks and control measures to mitigate them.

Recommendation 4

All health and social care organisations should provide evidence that they are taking action to improve cyber security, for example through the 'Cyber Essentials' scheme. The 'Cyber Essentials' scheme should be tested in a wider number of GP practices, trusts and social care settings.

As an exercise for improving security by targeting "low hanging fruit" this seems a sensible approach but it will not expose or handle any fundamental misunderstandings about information security management requirements and basics. Showing that improvements are happening runs the risk of ending up as "window dressing" if these improvements are not spreading awareness and promoting understanding.

Recommendation 5

NHS England should change its standard financial contracts to require organisations to take account of the data security standards. Local government should also include this requirement in contracts with the independent and voluntary sectors. Where a provider does not meet the standards over a reasonable period of time, a contract should not be extended.

Bear in mind the point about the data security standards being more directives and they should not be considered exhaustive. Contractual obligations are likely to help enforce good security practice but should not confuse existing protections in this regard.

Recommendation 6

Arrangements for internal data security audit and external validation should be reviewed and strengthened to a level similar to those assuring financial integrity and accountability.

Strengthening of audit is a welcome proposal, albeit occasional external audit should be considered. However the processes being audited are for health and social care – is financial integrity and accountability sufficient?

Recommendation 8

HSCIC should work with the primary care community to ensure that the redesigned IG Toolkit provides sufficient support to help them to work towards the standards. HSCIC should use the new toolkit to identify organisations for additional support, and to enable peer support. HSCIC should work with regulators to ensure that there is coherent oversight of data security across the health and care system.

Again what is needed here is an understanding of information security fundamentals across the organisations. We welcome the proposals to expand the functionality of the IG Toolkit to share expertise and encourage an educational approach, but it must be handled in such a way as to encourage understanding and collegiate working, not embellish or confuse existing organisational approaches and standards.

Recommendation 9

Where malicious or intentional data security breaches occur, the Department of Health should put harsher sanctions in place and ensure the actions to redress breaches proposed in the 2013 Review are implemented effectively.

Recommendation 10

The case for data sharing still needs to be made to the public, and all health, social care, research and public organisations should share responsibility for making that case.

As stated above, the Farr Institute 100 cases provide a perfect illustration of why and how data sharing is important and save lives. ADRN – in the wider context of administrative data and the role of public authorities – raises similar issues. Research in these contexts about the likely causes and effects of ill health and poor well-being, seen as part of an holistic social picture, requires more joined-up-ness of standards, best practices, information governance interoperability and public engagement.

For more on the work of the ADRN, see: https://adrn.ac.uk/

Recommendation 11

There should be a new consent/opt-out model to allow people to opt-out of their personal confidential data being used for purposes beyond their direct care. This would apply unless there is a mandatory legal requirement or an overriding public interest.

We understand the politics behind this particular policy approach. At the same time, we are concerned not to establish a system that fetishes consent at the expense of other important public goods, such as the conduct of scientifically-sound, ethically robust research. The tone of the Review suggests that the bar will be set very high if reliance is to be placed on an overriding public interest to fore-go an opt-out, see para 3.2.40. While, once again, this might be politically expedient, we would seek assurances that the same expectations of public interests will not bleed into other contexts where appeals to the public interest to further research are already made and robustly defended. The prime example here is the work of the Confidentiality Advisory Group. In most of their work, there is not a request to override an opt-out but rather to proceed without an explicit, specific consent. Might we therefore see multiple standards of "in the public interest" developing? If so, how will this be managed and communicated and given appropriate effect?

Questions arise as to how the new consent/opt-out model would be implemented and how practicable it would be. Some are presented here: How would be model be resourced? Where would the individual choices be made and registered? Would there be a central register of opt-outs? How would a change of mind be conveyed and enacted after data have been shared? Assurance is to be given to individuals that their choice will be respected, but is it practicable? Would there be an effective date for each change of mind? Would the profile of opt-outs be conveyed to data users so that any bias was known? Is it acceptable to have one grouped choice for data sharing across health and social care organisations when focus group work stated that there should be consent for a social worker to access medical records (ref. 70)?

Recommendation 12

HSCIC should take advantage of changing its name to NHS Digital to emphasise to the public that it is part of the NHS 'family', while continuing to serve the social care and health system as a whole.

We entirely concur.

Recommendation 13

The Government should consider introducing stronger sanctions to protect anonymised data. This should include criminal penalties for deliberate and negligent re-identification of individuals.

Please see our response above to Recommendation 9. If stronger sanctions are to be applied in this context, what else is envisioned beyond deliberate and negligent re-identification of individuals? Note, for example, as stated above, there is a world of difference between deliberate and careless conduct. We question whether negligent conduct alone should be covered, unless this is tantamount to gross negligence. Moreover, beyond re-identification will attempts also count? And beyond misuses of anonymised data that have (potential) privacy implications, what else is envisioned?

If the intention is to emphasise that anonymised data requires careful handling then this should be communicated in language more clearly associated with risk of re-identification and the need to ensure that a "blank cheque" for use and processing cannot be inferred by controllers and handlers of the data.

There is a need to maintain a balance. Data collected as part of health and social care is invaluable for direct care and wider purposes. Along with the idea of stronger sanctions for deliberate and negligent re-identification of individuals, comes the risk of increasing fear of data sharing. It is not always straightforward to determine if an action was deliberate and/or negligent, and, as we have noted, the most frequent problem is IG maladministration. Greater awareness and understanding will be the key.

Case Study 9: UK Biobank

We would point out that while the example of UK Biobank is indeed an illustration of explicit consent, this is more particularly an example of broad consent. That is, participants sign up to participate in UK Biobank broadly as a research endeavor to build a research resource for health-related research. Participants did not know at the time what specific uses their data and samples would be put to, to which ends, or by whom. This is only ethically acceptable because there is robust oversight in the guise of the independent Ethics and Governance Council. People are not fully informed at the time of recruitment. It is important to tease out the contours of such different forms of consent. Equally, withdrawal from UK Biobank will not necessarily result in destruction of all data or samples – only to the extent practicable at the time. The key message here is that participants' expectations cannot be left to consent/withdrawal alone.

Recommendation 15

People should continue to be able to give their explicit consent, for example to be involved in research.

Following from the above, it will be important to be clear here that 'explicit' consent need not mean 'specific, informed' consent in the sense that all risks, benefits, burdens, and alternatives need to be known and disclosed at the time of giving consent. This is potentially disingenuous as it would not be possible to achieve this at the time of giving consent, let alone be sufficiently

People should also have a greater opportunity to be involved with the governance of data that is being processed on a sound legal basis, whether that involves consent or not. Their involvement should not be limited to providing consent alone – there must be an opportunity for them to articulate their expectations and wishes, as well as have a handle on deciding how publicly funded research is designed, developed, implemented and governed.

Recommendation 16

The Department of Health should look at clarifying the legal framework so that health and social care organisations can access the information they need to validate invoices, only using personal confidential data when that is essential.

While we agree that legal clarity is important, it is not always sufficient to deliver sound governance. The case in point is care.data which was perfectly 'legal' because of the Health and Social Care Act 2012, but this did not prevent the significant social backlash. We have argued elsewhere that the failure to secure 'social licence' was a big driver in the failure of this initiative. The law is but one part of the picture in this landscape.

See further here: http://jme.bmj.com/content/early/2015/01/23/medethics-2014-102374.full.pdf+html

Recommendations 17 and 18

Recommendation 17: The Health Research Authority should provide the public with an easily digestible explanation of the projects that use personal confidential data and have been approved following advice from the Confidentiality Advisory Group.

Recommendation 18: The Health and Social Care Information Centre (HSCIC) should develop a tool to help people understand how sharing their data has benefited other people. This tool should show when personal confidential data collected by HSCIC has been used and for what purposes.

We entirely endorse these recommendations. We would add further – returning to our earlier comment about the crucial importance of a regulatory stewardship role – that both organisations could usefully do more to flag their contribution to such a role for potential data users/sharers in assisting them to a position of preparedness.

Recommendation 19

The Department of Health should conduct a full and comprehensive formal public consultation on the proposed standards and opt-out model. Alongside this consultation, the opt-out questions should be fully tested with the public and professionals.

We support this Recommendation and suggest that the refinement of any formal consultation could benefit from some of the comments made herein. We emphasise the importance of framing the consultation carefully. However often we ask about the acceptability of data use, there will be a proportion of people who are not in favour. It will be necessary to present not only the benefits of data use, but the harms due to the non-use of data to create the fuller picture. This was a component of our commissioned work for the Nuffield Council on Bioethics.

Recommendation 20

There should be ongoing work under the National Information Board looking at the outcomes proposed by this consultation, and how to build greater public trust in data sharing for health and social care.

We refer once again to the opening statements of this response. We believe that it is a fallacy to talk about building trust. Dame Fiona's opening words more accurately reflect the challenge: to demonstrate trustworthiness.

THE CONSENT/OPT-OUT MODEL

On the Eight Point Model

Point 1: what is meant by "allowed by law"? Must this be an explicit legal (statutory) gateway, or might the existing common law be sufficient?

Point 4: we favour the two options approach for the principal reason that care functions might otherwise be jeopardised if people only have one option to opt-out and they do so for non-care reasons, such as a distaste for research.

Point 7: it should be recognised that no mechanism or method of anonymisation is entirely risk-free. Techniques are more a craft than a science. Citizens' expectations should be set accordingly.

On the four opt-out proposals

We do not favour either 3 or 4 for the reason stated above. Number 1 leaves unanswered questions around the difference between the categorise of 'Limited' and Restricted': the terminology is unclear. Number 2 presents the initial information well, but the options themselves are poorly worded, in particular there are too many 'do not' statements that are potentially confusing.

Although the four options are, at this stage, delving into the detail before the principles are properly established, it will be very important to consider how the information is presented and how the questions are asked. It would be advisable to pilot possible layouts to see how they themselves affect the responses. It is possible that people will feel the need to choose an option. It would be unfortunate if the mechanism proved to be a stumbling block to the message.

General observation on the methods used in the report: we note that in some cases the evidence is based on fairly small numbers of participants, sometimes individual views. Judging from their description, the on-line survey respondents might not be representative of the population.

In summary, we welcome the review and support its emphasis on trustworthiness in data sharing. This work will play an important role in the future of data sharing and use, and the next steps need to be carefully planned to ensure they contribute to an appropriate balance between safeguards and the promotion of data usage for public good. Greater awareness and understanding of existing measures are needed, and work with the public requires openness and wisdom. The Farr Institute welcomes the option to contribute at later stages of the consultation process.