Cancer Research UK Response to the National Data Guardian's review of Data Security and Consent

September 2016

Key points

- Cancer Research UK welcomes the publication of this Review and the Department of Health's consultation. We are glad to have the opportunity to respond and look forward to working with the Department and others on the implementation of the recommendations. We have submitted additional evidence through our Review of Informed Choice for Cancer Registration in partnership with Macmillan Cancer Support. This response therefore does not specifically relate to the cancer registry as a dataset but covers a broader range of issues.
- We support the ten new security standards, which represent a welcome step in the right direction for data management in health and social care; we hope they will help promote consistency and build public trust. Implementation of the standards should be considered as part of a wider piece of work, examining and addressing the systemic issues leading to data breaches and wider data insecurity.
- We also support the new consent model and the desire for a simple system; of the two options proposed we strongly believe a single opt-out is the best option. However, we have outstanding concerns about some of the terminology used in the proposed model and would therefore welcome clarification or further guidance.
- We strongly recommend that a thorough programme of user testing is carried out on these proposed models, with members of the public who have not been previously engaged with these issues.
- We would welcome further detail on how NHS Digital will ensure coherent oversight across the whole health and social care system, as well as on the division of responsibility between NHS Digital and the CQC. We are concerned that resource within NHS Digital will be a limiting factor in the success of this work and encourage the Department to consider whether any additional resource is required.
- The success of this model will depend on its implementation. The security of the system must be ensured and careful communications planned before any opt out model is presented to the public. The Department of Health should publish a clear timeline for implementation, including key intermediate milestones to be met before the new model is presented.

General comments

Patient data is essential for improving outcomes for people with cancer – through research, as well as improving cancer services. Cancer Research UK currently has 38 active research grants which directly rely on access to data sets and linkages, as well as a large internal analysis and evaluation team who carry out statistical analysis; both independently and in partnership with a range of health and social care organisations.

It is important that people with cancer, and the wider public, are informed about how their data is used and their rights to opt out of data sharing. We were pleased to see the Review's focus on improving public communications on data. As part of our own consultation to inform this response, we held a three-hour workshop with patient representatives from Cancer Research UK and the British Heart Foundation, who we consult quarterly to inform our data policy work.

We are glad to have the opportunity to respond to this consultation on the National Data Guardian review. In addition to this response, we have submitted a joint response with Macmillan Cancer Support as the 'Review of Informed Choice for Cancer Registration'. We would be pleased to discuss any of the issues raised in either response further if that would be helpful.

The 10 Security Standards

We support the intent of the 10 proposed standards and the ambition to support rather than limit data sharing; we hope their implementation will help promote a consistent approach to data management across the sector. In order to ensure that their intent is realised, it is important that individuals and organisations are supported to implement these standards and that staff are encouraged to learn from near misses.

There must be a balance between personal and organisational accountability, as well as acknowledgement and action when systemic issues are causing breaches. We are concerned that these proposals lean too heavily on personal accountability – especially in light of the review's evidence of the organisational factors that lead to staff members taking 'workarounds', and the reliance on Trust or University IT departments to maintain secure and functional systems.

Our concerns are as follows:

- From a research perspective it is possible that an increased focus on personal accountability could make the health sector less appealing to data analysts, furthering existing challenges with recruitment. This is especially evident in combination with new criminal penalties being introduced.
- The phrase 'deliberate or avoidable breaches' puts a system-driven workaround in the same category as a malicious leak. We encourage the review team to explore alternative wording which would reflect the intent and seriousness of the breach. At the least, we would welcome a more precise definition of this phrase.
- The standards must also be meaningful to the patients whose data they intend to protect. When we tested these standards with patient representatives, they were not wholly reassured and felt that without system-level change behind them, the standards would not be effective. We understand that some of these issues will be addressed by the Wellcome Trust taskforce and look forward to engaging with their programme of work over the next two years.

Implementation of the security standards: Cancer Research UK

These security standards are important to Cancer Research UK as an organisation, both as a funder of medical research and as an organisation with an internal analytical team.

At present, our internal analysts do not use personal confidential data. However, we are in the process of acquiring IG Toolkit accreditation for our Analysis and Evaluation team in order to enable a wider program of work. Through this process we hope to ensure our compliance with these standards. However, there are several outstanding areas of concern.

Standards 1-3: We would appreciate clarity on how far–reaching these standards are, which refer to all-staff; whether this has a literal meaning of all staff within that organisation, or whether this could be limited to research teams using personal confidential data. We believe the latter option, as followed by the IG Toolkit accreditation process, is more appropriate in this case.

Standard 3: We would also welcome further detail on whether Standard 3 would be applied retrospectively; this could result in a substantial backlog and delays in analytical projects across the sector. Annual training and mandatory tests must be readily and regularly available to new starters, so as to avoid bottlenecks in recruitment; there should also be clear ways for staff to raise concerns or seek advice as necessary between training sessions.

Standard 4: Researchers using personal confidential data are already required to delete data after use, in accordance with NHS Digital's standard contracts. However, it would be difficult to implement attributing access to individuals. For many researchers this may necessitate procuring new software, which could in turn lead to compatibility issues with existing software.

Standard 8:

- This would benefit from a clear definition of 'unsupported'; applying a strict definition across a whole IT estate seems unnecessarily broad and may cause difficulties for many organisations since some legacy software will only run on older web browsers.
- Furthermore, open source software is widely seen as the direction of travel for research, and is regularly used. There is therefore concern that this Standard could stifle innovation.
- Standard 8 has further implications for remote workers. The tracking software required for Standard 4 to be implemented might be incompatible with VPNs, which sometimes scramble or hide IP addresses. This may make collaborations more difficult and could make such roles less accessible.

Implementation of these standards may be difficult, since researchers would be reliant on their institution's IT support, for whom this may not be as much of a priority. Ensuring compliance is likely to be time- and resource-intensive and could result in a loss of flexibility for academics in how they carry out their research.

Implementation of the security standards: health and care organisations

The most significant issue for health and care organisations in implementation is not the standards themselves, but the underlying issues forcing staff to take insecure 'workarounds'. The review gave a strong example of such a case, about temporary staff using others' log-ins or passes in order to access hospital systems.

The above example could be considered a deliberate and avoidable breach. However, if the limiting factor is the Trust's technology, the alternative would be not accessing the system at all – which might lead to confidential information being stored in a less secure way, such as written on paper. This could incur a later clinical risk, as vital information is missed. This workaround should not happen whatsoever, but the focus should be on making Trusts responsible for addressing the underlying issue as well as individuals. We would welcome alternative phrasing that makes a distinction between this type of breach and one that is carried out with malicious or negligent intent.

We have also noted that the effectiveness of Caldicott Guardians in Trusts is variable; owing to varying levels of engagement and a mixture of job roles holding the Caldicott Guardian title. It would be helpful for the Department of Health to clarify their mandate, in order to ensure that they have 'teeth' in the organisation and can effectively promote the new standards.

New approaches to objective assurance

We support the inclusion of data security standards into CQC inspections. However, it is not clear how NHS Digital would use the refreshed IG Toolkit to inform the CQC of 'at risk' organisations. In

addition, it must be noted that there is no equivalent for non-NHS organisations that process personal confidential data – such as universities, commercial companies or organisations such as Cancer Research UK with internal analysts. We would therefore welcome clarity about how compliance with these standards will be assessed.

Our external researchers are expected to adhere to the highest standards of research rigour and integrity, in line with the Universities UK Concordat to Support Research Integrity[1] and with host institutions' policies. This is included as part of our standard grant conditions[2] and covers responsible handling of sensitive data, and safeguards for privacy and confidentiality. Further safeguards are in place for clinical trials.

Beyond this, the Health Research Authority (HRA) could play a role. The HRA maintains the Research Governance Framework for Health and Social Care[3], which researchers must adhere to, and reinforces the need for studies to have appropriate approvals in place from Research Ethics Committees. The Framework also states:

> *"The appropriate use and protection of patient data is also paramount. All those involved in research must be aware of their legal and ethical duties. Particular attention must be given to systems for ensuring confidentiality of personal information and to the security of those systems."*

Given these significant differences in assurance we would welcome further detail on how NHS Digital will ensure coherent oversight across the whole health and social care system, as well as on the division of responsibility between NHS Digital and the CQC.

Further guidance on implementation for Trusts and other organisations would be helpful in the light of this ambiguity. This should be clear, but should be flexible enough to allow organisations to design their own solutions for implementation. This is crucial given the breadth of organisations that process health and care data.

We also support the refreshing of the IG Toolkit and the removal of self-assessment. External assurance will make accreditation more robust, ensure compliance with the new standards and promote confidence in the organisations holding IG Toolkit accreditation.

In terms of peer support, it may be more effective to pair non-compliant organisations with compliant organisations so that they can learn from them.

Stronger sanctions

We strongly support the principle of introducing stronger sanctions to protect anonymised data, especially in the light of NHS Digital planning to release more anonymised data: this will help promote trust in the system. This must be communicated with a caveat that it is impossible to completely remove the risk – especially when considering linked or genomic data.

We would welcome clarity on where responsibility lies for monitoring and policing deliberate re-identification. In Cancer Research UK's grant conditions, the onus is placed on the university to ensure good scientific conduct and to inform us as the funder of any alleged misconduct – including a data breach. Cancer Research UK would then terminate funding to that research group. We

[1] The concordat to support research integrity, Universities UK, July 2012
[2] Cancer Research UK standard grant conditions
[3] Research Governance Framework for Health and Social Care, Department of Health, 2005

recommend that this responsibility is held by the host institution rather than a funder, since it would be impossible to remotely police this.

The consent model

We support the general trend of moving towards more anonymised data releases, with NHS Digital acting as a statutory safe haven. We also support and recognise the need for a simple system that is understandable and meaningful to the public as well as to those heavily involved in the area.

However, there is still work to be done to ensure that this is intent is realised. It is vital that any proposed model is thoroughly user-tested; not just with those who have existing health conditions and are already engaged with these issues but with members of the public from different backgrounds who may have very little pre-existing knowledge of patient data.

The eight elements of the consent model

An overarching question remains about the purposes of these eight statements and how they will be presented to the public. A fundamental part of this is ensuring that the materials are understandable and meaningful to the general public and the average level of literacy. 16 per cent of UK adults have literacy levels at or below those expected of an 11 year old; it is therefore important that any communications must be clear, unambiguous and written in basic English.

A number of phrases in the new model would benefit from a clearer definition, including:

- *'Personal confidential information'*: this is not likely to be a meaningful phrase to most people and from a technical perspective does not have a widely recognised definition.
- *'Other beneficial purposes':* Some useful examples of such beneficial purposes are given under point 4; these should be more clearly linked to this point.
- *'Overriding public interest':* we would welcome clarity on its definition, as well as how this is decided and by whom.
- '*Consent*': this implies an opt-in system rather than opt-out. This may cause misunderstanding and concern, since there are many uses of data where gaining consent will not be necessary.
- *'Others involved in providing your care'* is also ambiguous. We know from the Wellcome Trust's research into commercial access to data[4] that when private companies are involved in providing care it is of utmost importance that the rules governing that access are clear and well-communicated, and that decision-making is transparent.
- '*Anonymised*': Although some data is truly anonymous, it is very difficult to completely remove the risk of re-identification. It may be safer to use a term that is not so strong, such as 'de-identified'. The precise language used should be developed as part of the Wellcome Trust taskforce's work.
- '*Regulators and those providing care checking its quality'*; this presumably refers to clinical audits, but to many this may seem contradictory to the later point stipulating that the opt-out does not apply to the Care Quality Commission.

The proposed opt-out models

[4] The One Way Mirror: Public attitudes to commercial access to health data, Wellcome Trust, March 2016

We have a strong preference for a single question opt-out. The distinction between research and improving the NHS is often a blurred line; many service improvement research projects would fall somewhere in between. Applying opt-outs to a two-question model would be extremely confusing for data holders and would likely create issues when planning research that falls between the two. In essence, this presents the public with a choice that would be impossible to implement fully.

Furthermore, given the public's concerns about commercial access to data, there may be an assumption that opting out of medical research will also mean opting out of commercial access entirely – which is not true. This preference was shared by our patient panel, who saw the single question option as simpler and more easily understandable.

There was less agreement about whether information profiles or tick boxes were more understandable. The patient group felt that the tick box statement was confusing, since they were being asked to tick if they did *not* agree with the statement. Although they preferred the look of the information profiles, they were unsure about how this model could be presented unless it was online. A suggestion was to use the wording in the information profile, but with a tick box next to each rather than a circle to be clicked.

We recommend removing the example of charities evaluating the quality of services. We recommend focusing on examples from the NHS or medical research instead.

We strongly recommend that a thorough programme of user-testing is carried out on these proposed models. This should be done with people who have not been previously engaged with a charity, with research or with the healthcare system, but with focus groups made up of members of the public from a wide range of backgrounds.

Implementation of the consent model

Ahead of implementation, NHS Digital must produce clear guidance, including a clear timeline and the status of previously-registered Type 1 and 2 objections. Clear communication about any decision made on these objections is essential. When the Type 1 and 2 objections were implemented in early 2016, there was significant confusion about which datasets and releases would be affected and the official guidance raised more questions than it answered. Although we have had good direct engagement with NHS Digital about these processes, we are aware that others without such a good relationship with them may have found this very confusing.

In order to minimise the effect of such changes to longitudinal research studies, there must be means by which researchers can assess the impact of applying opt-outs, and the demographic breakdown of those opt-outs. This will help minimise bias. It would be helpful if NHS Digital assisted with this, and will become more important as sanctions for re-identification are introduced. At present, NHS Digital have offered to work with researchers to assess the impact. While very welcome, this is not a sustainable solution considering their limited resource.

In order to implement this model effectively, it is vital that NHS Digital is sufficiently resourced. Although we have seen improvement in their data release processes, we are concerned that implementing this new model will be extremely resource-intensive, perhaps prohibitively so in the light of a 30 per cent budget cut by 2020. We would welcome reassurance from the Department of Health that NHS Digital will be adequately resourced to carry out these new responsibilities.

For further information please contact Rose Gray, policy adviser on 020 3469 8046 or rose.gray@cancer.org.uk

About us

Cancer Research UK is the world's largest independent cancer charity dedicated to saving lives through research. It supports research into all aspects of cancer and this is achieved through the work of over 4,000 scientists, doctors and nurses. In 2014/15, we spent £434 million on research in institutes, hospitals and universities across the UK. We receive no funding from the Government for our research and are dependent on fundraising with the public. Cancer Research UK wants to accelerate progress so that three in four people survive their cancer for 10 years or more by 2034.