BIG BROTHER WATCH
DEFENDING CIVIL LIBERTIES, PROTECTING PRIVACY

National Data Guardian for Health and Care's Review of Data Security, Consent and Opt-Outs – Big Brother Watch Response

About Big Brother Watch

Big Brother Watch is a civil liberties and privacy campaign group founded in 2009. We produce unique research which exposes the erosion of civil liberties in the UK, looks at the dramatic expansion of surveillance powers, the growth of the database state and the misuse of personal information.

We were a member of care.data advisory group and gave oral evidence to the Health Select Committee on the scheme. We have also produced FOI reports on the number of data breaches suffered by NHS bodies.

We are responding to this consultation in a professional and public capacity.

Response

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

We welcome the attempt to create a set of security standards and acknowledge the effort made to address fundamental concerns regarding data security within the NHS. However, greater clarity of some of the standards is still needed in order to ensure patients fully understand what the security measures are for their personal information.

Standard 1: The lawful and appropriate purposes for sharing personal confidential data should be clearly defined.

We draw attention to this as we are profoundly conscious that the introduction of the Digital Economy Bill; in particular Part 5, will either create potential new data sharing capabilities or will relax existing "gateways", with the intention of enabling easier and potentially greater sharing of data between Government departments.

There are currently no published plans to use health or medical data, but it would be naïve to presume that plans to use this data will not appear in the future.

The intention to use health or medical data to improve services, to improve the "wellbeing" of citizens or for the purpose of "national security" must be made clearer.
We raise this in light of the recent Supreme Court ruling on the Named Person Scheme in Scotland which stated that "wellbeing" is too low a bar for data to be shared. There must be consensus that the appropriateness outlined in the NDG's review is relevant and does not unduly or unnecessarily breach the privacy of the individual. Spurious use of personal identifiable data does not tick the appropriate box.

Furthermore the debate relating to medical records being excluded from bulk personal datasets in the Investigatory Powers Bill[1] must be considered. It is one thing to use health data to protect national security in the face of a health epidemic; it is quite another to use individuals medical or health records as a targeted or bulk surveillance capability.

Definitions should be published as part of the proposed security standards in order to make exactly clear when personal confidential data can be shared or used, and what exactly is deemed to be "*lawful and appropriate*". Without clear definitions the opportunity to extend what is appropriate beyond the principles outlined in the review may occur, subsequently undermining the work of the National Data Guardian (NDG).

Standard 6: A clear and easily understandable description of the process when a data breach occurs would be beneficial. This would clarify exactly how a report is to be made and who - in addition to the proposed senior management - will receive the report, handle the problem and subsequently oversee the process.

We believe there would be benefit in involving an independent commissioner who has an expertise in data security, data breaches and data misuse. Their expertise would be a boon in assisting senior management in resolving the breach efficiently.

We are surprised that an annual audit is not outlined as part of this standard. An annual audit would be beneficial as it would ensure the reporting of the number of data breaches, as well as any incidents of misuse or hacking.
Ideally any audit would be undertaken by the National Data Guardian with the results being published as part of an annual report. By publishing a single report it would provide an easily accessible overview of how all the different bodies were approaching data protection. Having the National Data Guardian undertake audits and publish an annual report would also give a sense of independence to the process.

Standard 9: We acknowledge the reference to the Government's Cyber Essentials Scheme but it would be helpful if greater specific detail were provided which indicated clear that data will need to be encrypted, hashed and stored in secure data centres. Without exact guidance - supported by the Cyber Essentials Scheme more broadly - there is a risk that good intentions will be undermined and patient information will be left vulnerable.

Standard 10: There is no detail about how suppliers will be held to account. More information needs to be published to clarify whether or not suppliers will be subject to publicly published annual audits and what penalties suppliers will face if they fail to protect personal confidential information?

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?

"HSCIC should work with other regulators to ensure that there is coherent oversight of data security across the health and social care system."

[1] Investigatory Powers Bill, *Public Bill Committee: Twelfth Sitting*, 26th April 2016, http://www.publications.parliament.uk/pa/cm201516/cmpublic/InvestigatoryPowers/160426/pm/PBC_Investigatory%20Powers%2012th%20sit%20(pm)_26_04_2016.pdf

We support this intention but would like to see greater detail about which other regulators are being considered and what role they will play. It would be preferable if an independent, non-health care body, whose sole purpose was oversight and data protection, were on hand to assist HSCIC, rather than a body which looks at these areas as part of a broader remit.

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

Standard 4: The new definitions offer greater clarity than before, however we are disappointed with how narrow they are.

We do not support the view that citizens should not be able to opt out from sharing confidential information with studies conducted by third party researchers.

The recent revelation that Moorfields Hospital signed an agreement to share data with Google's DeepMind project without seeking explicit consent from patients is one example as to why informed consent in the form of an opt in is critical.

Furthermore it must be made clear to patients exactly what it is they are choosing to opt in or out of. Based on the definitions provided in the consultation document not enough information is provided for an informed choice to be made.

Standard 7: If anonymised data is not subject to an opt out, citizens must be informed that their data may be at risk of re-identification. To be clear, even if the risk is small, the citizen should be told.

We say this because we remain concerned about the weight placed on anonymisation as a fool proof and secure method of protecting people's identity. It is not. There is a wealth of research which shows that anonymisation does not categorically protect people from re-identification. We draw your attention to the work of the UK Anonymisation Network[2] . Their recent publications emphasise that anonymisation is merely a way of balancing risk; not removing the capability of identifying a person.

A 2015 study conducted by Professor Latanya Sweeny Phd (Professor of Government and Technology at Harvard University, Director of the Data Privacy Lab and former Chief Technologist at the Federal Trade Commission) proved that 100% re-identification was possible even when the data was anonymised. By taking the South Korean Resident Registration Number which closely matches the make-up of the UK's NHS number, Professor Sweeny was able to re-identify all citizens using two entirely different methods. [3] Professor Sweeny's ought to be assessed[4], because much of her work demonstrates that anonymisation is not without risk and cannot guarantee the security of personal information.

[2] UK Anonymisation Network: http://ukanon.net/
[3] Technology Science, De-anonymizing South Korean Registration Numbers Shared in Perscription Data, 29th September 2015: http://techscience.org/a/2015092901/
[4] Latanya Arvette Sweeney Ph.D: http://latanyasweeney.org/cv.html

Until a method is discovered which makes re-identification at least 99.9% impossible we will continue to oppose the use of anonymised data for non-legal purposes outside of an individual's direct medical or social care.

Because of the issue of re-identification, the sharing of identifiable personal data for the benefit of a statistical authority is an area of profound concern. We are particularly concerned about the intention to share NHS numbers and addresses with the Office of National Statistics (ONS). Given that an NHS number and address is specific personal data, the citizen should have the choice to opt out of its use for statistical purposes.

Greater detail must be provided regarding what data will be shared and how. Information on whether the data will be encrypted, hashed and stored in secure, non-cloud data centres has to be made available. Finally, if the wider intention is for the data to be shared with other Government departments via new "gateways", as referred to in the Digital Economy Bill, this must be made clear and an opt out must be offered.

Whichever model is decided upon, time should be set aside for full scrutiny by anoymisation experts such as the UK Anonymisation Network, data scientists and anonymisation practitioners.

Finally, whilst not specifically relating to the statements per se, we have concern at the lack of reference in any of the consultation documents or the NDG's review to what rights the citizen has to access their own data.

The consultation appears to offer control to the patient, but deeper reading reveals that the patient has little to no control over their own data and no real defined power to access it. There is no indication how data should or could be shared with the patient, what rights of access the patient has to their medical or health data, or in what form the patient can receive or view their data.

We note that information on how a patient can access their medical records is due for renewal in 2017[5]. Information about patient access and control should be included, not only in the proposed consent model, but also as part of the Data Security Standards. This will help give clinical professionals clarity about which data protection requirements will apply if a patient requests access to their own data.

We raise this as a concern which has long term consequences, particularly as it is anticipated that as the digitisation of society progresses there will be a greater shift towards the individual having data ownership and control over decisions made about their data.

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?

Yes, as the NDG Review acknowledges *"there are problems involving people, processes and technology. Data is not always adequately protected and individuals and organisations are not consistently held to account."*

[5] NHS Choices, *How do I access my medical records (health records)?*, 21st July 2014: http://www.nhs.uk/chq/pages/1309.aspx?categoryid=68

Our unique research, based on Freedom of Information requests, supports this statement. In our November 2014 report "*NHS Data Breaches*"[6], we revealed that between 2011 and 2014 there were at least 7,255 data breaches in the NHS; the equivalent of 6 breaches a day.

With the huge increase in data citizens and organisations now generate, a new model of data handling must be designed and implemented. Furthermore sanctions available to punish those that misuse personal information must be strengthened.

It is now generally agreed that a fine is no longer a sufficient deterrent for those who intentionally misuse personal information and that custodial sentences are now needed to curb serious breaches. This is a view which has support from the Science and Technology, Home Affairs and Justice Select Committees, the findings of the Leveson Inquiry and the Shakespeare Reviews as well as the Information Commissioner's Office.

The measure could be quickly implemented as the power to punish serious breaches with a two year custodial sentence is already present in Section 77 of the Criminal Justice and Immigration Act 2008.

Serious breaches of data protection should be punished with a criminal record. It is unacceptable that an individual could cause a serious data breach, leave their job and potentially be employed in another role where they have access to large amounts of personal information.

Whilst stronger sanctions are one solution, they must not be seen as the only solution. Creating an environment of fear will not create better data protection methods.

Dame Fiona Caldicott outlines the need for a new improved approach to data. We support the need for strong leadership from the SIRO scheme but we would like to see independent oversight which is separate to HSCIC or NHS Digital to ensure absolute transparency of process if an error, breach, hack, misuse were to occur.

It's also important that those working in the NHS properly understand their responsibilities to the personal information of patients and how to keep it secure. Too often we see breaches occurring because of carelessness or simple mistakes. This can be avoided by ensuring that the data protection training employees receive is of a consistently good standard.

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

The now defunct care.data scheme created a great deal of confusion for patients and service users. We welcome a concerted effort to improve public awareness and engagement. However we don't believe the assertion that people were confused because of the complexity of the scheme. We would argue that the confusion was caused by the repeated changes to what the scheme would have permitted and the poor public awareness campaign, most notably the infamous "pizza leaflet" incident.

[6] Big Brother Watch, *NHS Data Breaches*, November 2014: https://www.bigbrotherwatch.org.uk/wp-content/uploads/2014/11/NHS-Data-Breaches-Report.pdf

The new consent/opt-out model must not dumb down the options for citizens. Citizens are asked to make decisions about their data on a daily basis now. Whilst some people may find it confusing it is a fact of life that decisions must be made. Downplaying or assuming citizens do not want to be asked complex questions does a disservice to the general public and undermines the importance personal data has to the individual.

An honest, straightforward and detailed explanation should be presented to the general public. The language must not prioritise either the perceived advantages or disadvantages of the options. It should be completely non-judgemental and simply explain what the options are. The model must not be seen as an opportunity to nudge patients towards a particular objective. In this manner patients decisions will be their choice, furthermore it will be an informed choice based on clear, neutral, honest and factual information.

As a starting point we would expect to see a large scale public awareness project take place. This should utilise every medium including television, print, social media and public billboards. We would also expect to see literature, including posters, to be clearly displayed in hospital, clinic and GP reception areas and at pharmacies and chemists. We appreciate this would be a costly procedure but the short term cost implication would, we believe, result in greater long term impact of awareness and engagement than a one off leaflet pushed through the door.

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?

Creating a coherent and honest framework which has independent oversight and offers choice to citizens is critical. We are encouraged but continue to have concern that there remains no opt out for citizens who do not want their personal information to be used for purposes beyond their individual direct medical, health and social care, for example research or statistical purposes.

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?

Yes. Anonymisation is not a fail-safe way of protecting anyone let alone “affected persons”. We are conscious that data sharing has the potential to enable profiling. When data is shared with other Government departments, as is being proposed in Part 5 of the Digital Economy Bill and in the form of bulk personal data sets under the Investigatory Powers Bill, there is an inevitable impact on citizens’ personal privacy and security.

Health and medical data is one of the particular areas the general public can feel very nervous about sharing or permitting access to. Not allowing a citizen to opt out of their data being shared outside of the health and social care services does little to fully address some of the concerns “affected persons” may feel about eyes on their personal data.

Furthermore we are aware that the Office of National Statistics, have proposed using sensitive data to conduct what could be seen as non-essential statistical research, the Big Data Project 2015 is one example. This project proposed taking people’s names to determine their ethnic origin, intentions to use private smart meter data to determine when a house is unoccupied and using location data from

mobile phones to inform on population behaviour[7]. These proposed studies all have profound moral and ethical concerns and could provide an insight into the lives of citizens which has a "creepy" quality. This could also expose protected characteristics to ethically unsound statistical research whilst making sensitive data vulnerable.

[7] Office for National Statistics, *The ONS Big Data Project*: http://www.ons.gov.uk/aboutus/whatwedo/programmesandprojects/theonsbigdataproject