Which?

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

Which? response to “Data saves lives: reshaping health and social care with data (draft)”

23rd July 2021

Following the publication of “Data saves lives: reshaping health and social care with data (draft)” on the 23rd June 2021 we would like to offer our thoughts on the visions and proposals outlined. We appreciate that the Department for Health and Social Care (DHSC) has published a survey for people and organisations to respond to, however we would prefer to communicate our thoughts in this written submission as we have a level of detail and nuance in our response that is not possible to communicate via the survey format. We trust that this will be a welcome addition and will complement the survey responses you receive.

Which? is the UK’s consumer champion. As an organisation we’re not for profit - a powerful force for good and here to make life simpler, fairer and safer for everyone. We fund our work mainly through member subscriptions. We are not influenced by third parties – we never take advertising and we buy all the products that we test. Which? works in pursuit of its charitable objects for the public benefit.

We began working on Health Data in early 2020 in response to an explosion in popularity of consumer health and lifestyle wearables, apps and services. Now, against the backdrop of Covid-19, UK consumers are more aware than ever of the role individuals’ data can play in personal and public health. Equally they are aware of the issues and nuances around data sharing; they care and want to understand and control how data about them is collected, with whom it is shared, for how long, and for what purpose. We believe there is a vast opportunity to leverage data from individuals, and if handled appropriately this data can improve healthcare - indeed the health of patients.

Moving to a world in which healthcare is data driven requires a careful shift: openness, transparency and engagement will be key to success. Which? has been working with a consortium of businesses and organisations in a Health Data Sandbox convened by data consultancy Ctrl Shift. Phase 1 of this project is complete and a report into the opportunities arising from a trusted Health Data ecosystem will soon be published by Ctrl Shift.

Infrastructure

Overall Which? welcomes the publication of the draft strategy. We welcome the intention by NHSX to look closely at the entire data ecosystem and interrogate the data infrastructure on which England's health will rely in coming years.

The intention in the draft strategy to look at the current data architecture is welcome particularly in relation to the proposals to integrate consumer data into peoples' primary healthcare, which will absolutely rely on the foundations of data collection, use standards, security, privacy and quality and the entire data ecosystem being fit for purpose.

Papering over the cracks will not suffice for the loftier ambitions outlined in the draft strategy. The term "fixing the plumbing" is often used by data organisations to talk about building a digital and data ecosystem that works - we agree with the sentiment of this expression and expect to see further clear and unequivocal detail about how fixing the data plumbing across the NHS will be undertaken as the strategy develops.

Connectivity

If the intention of the draft strategy is to make healthcare digital and data driven, such ambitions will require everyone in the UK to be online and have a fast, reliable connection. This is still work in progress; indeed Which? has led the GigaTAG (the Gigabit Take Up Advisory Group) to accelerate the uptake of Gigabit broadband. For more information visit https://consumerinsight.which.co.uk/articles/gigatag

Whilst development and adoption of technology is important, tech-solutionism is a risk. Much of what is outlined in the draft strategy will rely on secure, reliable and accessible connectivity and devices, assumptions must not be made that these three things are easily available or attainable for all. Inclusivity will need to be addressed in order to ensure no one is left behind, not just the most vulnerable in society, but those who may be temporarily vulnerable due to challenging situations and circumstances based on their physical, mental or financial status at varying times in their life. We note that this is a concern for individuals as well as for organisations and businesses.

We would welcome detail as the draft strategy develops regarding what alternatives will be available for people who are unable to connect to digital health services or who choose not to access health services digitally.

The draft strategy also assumes that secure, reliable and consistent technology is available to all branches of the NHS's expansive operation and any third party suppliers involved. We would need to see clear evidence that this is true before we can back any move to make data transfer more open across the whole NHS estate. The risks to consumers' data if it is not secured are real and proven, so concerns over safeguarding these data must be central to any strategy that emerges.

Bringing people closer to their data

Chapter 1 of the draft strategy is a key area of focus for Which?. We welcome the intention to bring people closer to their data and the data about them but have a number of concerns about what that will look like in practice - most notably in relation to control, consent and transparency, the sharing of additional data and with whom data will be shared with more broadly.

Control, consent and transparency

The draft strategy states that people will have the ability to control and consent to how their data is used, yet there is no coherent detail given as to what control and consent will look like.

We note that there is reference to data stores such as the nascent SOLID project, discussion about people being able to see how their data is being used, through to statements about the need for data to be "made available for use". These are three very different processes, but they are all seemingly bundled together. There is a distinct lack of clarity about what data a person will be able to control, what data they will be able to consent to being used and what data will be made available for use.

Importantly, we believe that far more detail is needed as to what NHSX and more broadly what the DHSC are defining as "consent".

The current situation with the rollout of the GPDPR scheme has thrown the issue of consent into the spotlight, as the scheme is opt-out only and thereby assumes consent unless the patient signals otherwise. A survey undertaken by Which? revealed that of 1,700 people surveyed in July 2021 45% of them had not heard about the scheme. That's almost half of people who were unaware that their medical records were to be uploaded to the scheme, and almost half of people who had not provided any form of meaningful consent.

This finding also raises concern to the references of transparency in the draft strategy. Transparency, similarly, is not clearly defined. Is a poster in a GP's surgery and a webpage that very few people visit transparency working at its best? We don't think so. Our survey found that of the 55% of people who had heard of the scheme, only 12% had learned about it from a poster in a surgery and only 10% had heard about it via the website. The majority (32%) had learned about it from the news.

The concept of control is equally as unclear, other than the idea that a person may wish to use a data store or have the opportunity to upload data collected from a wearable or app or connected device to a medical record. This defined concept of control therefore seems to relate to data that a person collects themselves as opposed to the control of how data about them is being collected, shared, accessed or used within other systems or platforms.

As the strategy progresses we expect to see absolute clarity on what data will fall under these categories. What data will people be able to control, when will they have the opportunity to provide consent and indeed informed consent, and what data will be collected, shared, accessed, stored for wider use?

Future of data protection

The strategy references work by the National Data Guardian stating that when asked people say they are happy to share their data for secondary purposes other than their own care. It also quotes "as long as the legal and ethical safeguards are in place, people are ready to put their trust in the system to use their data for the wider public benefit, not just for their own care." We do not dispute this but understanding the nuance in these statements is critical when communicating with people and embedding the promises of consent and control. The legal and ethical safeguards being in place is one thing, but people will need to be clear on what they are and what their rights, this includes the right to redress if something goes wrong.

Under the UK GDPR, data can be used for research and science purposes and the legal and ethical safeguards are clearly outlined. We are curious why UK GDPR isn't referred to and these rights, opportunities and protections aren't outlined in the strategy. If the intention is for adaptation or development of the UK GDPR post Brexit it is vital this is clearly published and open for discussion with people and civil society as well as data protection, privacy, legal and ethics experts.

We raise this as the long term intention to embed AI into healthcare will require access to and use of data to enable machine learning and create algorithms. The rights that people will have to consent or to withdraw consent for collection and use of their data will need to exist and be clearly defined, communicated and embedded in data protection law as they currently are. This will be absolutely critical if the NHS wants to be trustworthy and have buy-in from the public. The right for people to say no is not something that disrupts innovation or development of products or services, as behaviours consistently show the majority are happy to contribute.

However there are a spectrum of reasons as to why a person may wish to opt out be it personal safety, religious reasons, cultural reasons, anonymity regarding a job they may have, or simply the choice not to be part of a data set. Enabling people to say no is as important as enabling people to say yes.

Equally, the NHS must justify why blanket consent is required here, and why technological solutions could not easily enable metered consent. Only people with a heart condition will have data relevant to a heart condition study, so the justification isn’t clear why everyone would need to consent to the possibility of this ‘just in case’. The pandemic has changed everything, but it is not a normative state and so should not be the basis for ongoing policy.

Whilst the NHS is a trusted organisation, trust should not be taken for granted. The 3.1 million people in England who have currently opted out of the GPDPR clearly do not trust how the NHS and the DHSC plan to use their data. We note this as a point of concern, not just in relation to trust but in ensuring that people's concerns and desire to know what, how and why their data is to be used are addressed and tackled in an open and honest way.

Sharing of additional data

The draft strategy refers to the opportunity for people to share additional data they have collected to "improve [my] wellbeing, such as sleep, food, exercise and genome" and the intention is for "allowing people to make their own contributions into that shared care record." Whilst this sounds positive in terms of engaging people with data in order to see its benefits, we must not be blind to the risks.

We must understand what measures need to be put in place to prevent harm and unintended consequences from the collection and use of poor, inaccurate or biased data. If the accuracy of the data collected is not of a high enough quality, the unintended consequences could be profound not just to patients' direct care, but as a challenge for GPs to be able to question and interrogate the data being uploaded so that they understand the full picture and how it relates to the patient not just taking the data at face value.

Commercial products

The consumer health, wellbeing and lifestyle market is booming with wearables and apps but there is a great muddle of language, of accuracy, of medical promises which aren't substantiated and of suggestions that monitoring of behaviours can lead to the prediction or prevention of medical problems. The line between consumer data (i.e coming from commercial apps) and patient data (ie medical records) is beginning to blur. The intention for data collected by commercial products to be shared into a persons' medical record and/or clinical care has great opportunity but poses a range of technical, security, data protection, accuracy and relevance challenges. Considering these and addressing the risks early will be necessary to protect people from potentially serious harm.

It is crucial that connected medical devices, commercial medical/health devices such as wearables and trackers, and commercial health, lifestyle, medical, wellbeing apps have high levels of security to protect patient's health and their sensitive data. Poor security practices such as weak or unencrypted passwords or lack of security updates pose a number of risks to patients. Leaking of sensitive data or a device not being able to function due to a ransomware attack can lead to patients experiencing anything from embarrassment to serious impacts on their health and wellbeing.

As we are concerned about issues of accuracy. We have undertaken testing which reveals that fitness trackers and smartwatches are regularly miscalculating the data they capture thereby providing inaccurate or misleading data to consumers. We have found an instance of a device miscalculating step count by 66%, meaning a person would only have taken 3,400 steps when it says they have taken 10,000 steps[1]. Discrepancies of such proportions could seriously mislead clinicians and patients and negatively impact on treatments and diagnosis.

Our tests also revealed that the heart rate monitoring feature in some fitness trackers and smartwatches was significantly inaccurate when compared to measurements from chest-belt monitors which are generally known to be more accurate than wrist-worn heart rate monitors. One device miscalculated the heart rate by 61%. Our testing also showed devices which are unreliable and inconsistent day to day. Reproducibility, or consistency, is just as important as accuracy. If a tracker is accurate on some days but not on others, consumers and their clinicians will not be able to trust it, and so will not be able to derive any meaningful insights from the measurements.

[1] https://www.which.co.uk/reviews/fitness-trackers/article/how-accurate-is-your-fitness-tracker-or-smartwatch-ad7fj7K6cFhz

These concerns are compounded as plenty of devices fall into a pseudo-medical sphere, yet are available to buy for consumers, such as pulse oximeters, blood pressure monitors, blood glucose monitors and even devices to take an electrocardiogram (ECG). Some of these devices are internet-enabled, meaning there are also security and privacy concerns involved.

The lack of regulation beyond self-regulation by the industry is also seen in the apps and services market. We have found that the security and data protection of many of the most popular apps - including ones recommended by clinicians - is of serious concern. A recent Which? investigation[2] revealed some of the leading apps and wearables including Sleepcycle, Babylon, Weight Watchers and others have poor data privacy practice and/or weak security. In one particularly alarming case[3] we found that the popular Wonder Weeks parenting app was hosting its baby monitor service on an insecure server based outside the EU that was also being used by gamers playing Minecraft. The security of the service was so poor, any unrelated third party could potentially snoop on the feed coming from a connected baby monitor used by parents for their peace of mind. This has thankfully now been fixed following our intervention.

Innovation

We welcome the intention within the draft strategy to work with innovators and the intention to look at standards and algorithms. We hope that this will be across the board including consumer and commercial products that the NHS want to see enabled to be interoperable and engage in data portability with NHS systems.

We support the plan to explore security and safety risks in medical devices and are happy to share intelligence from our investigations with the Medicines and Healthcare Products Regulatory Agency (MHRA), National Cyber Security Centre (NCSC) and NHS Digital as they engage through the Connected Medical Device Security Steering Group.

Furthermore we would be happy to collaborate and work with you on discussing the protections and clarity for the consumer as patient and patient as consumer as work progresses.

Security

We are encouraged by the statement that "our biggest weapon in staying ahead of the cyber threat is ensuring that we have security baked into the design of everything we do." But we don't see much evidence of this running through the draft strategy. We see a lot of efforts to make data more easily accessible, but not much detail on how it will be secured, in both primary NHS organisations and affiliates. Clarity on how security by design will be baked in is critical, so that it can be understood and interrogated as necessary.

Furthermore, we would be keen to see plans for how data and systems will be audited -

[2] https://www.which.co.uk/news/2021/06/fit-for-purpose-the-health-apps-that-pose-security-risks/

[3] https://www.which.co.uk/news/2021/06/popular-baby-monitor-app-put-privacy-at-risk/

potentially by a credible independent body - to ensure that security by design and privacy by design are being handled and if they are being maintained. Ongoing oversight of systems and data usage will be another area that will embed and build trust with consumers and patients.

How data is handled

We welcome the discussion around Privacy Enhancing Technologies in relation to how data is handled and we note that the Centre for Data Ethics and Innovation have recently published their BETA on PETs which is a useful addition to the conversation. These are clearly interesting approaches to the usability of data sets in a privacy enhancing way. We look forward to seeing how they advance. However we are concerned by the language around pseudonymisation that is coming through from the GPDPR, most notably that patients could be reidentified at any time if it is deemed for a legitimate reason yet the legitimate reasons are not clearly explained.

If the NHS is serious about wanting people to better engage with their data and share data for reasons beyond their individual care, there is work to be done on explaining to people the difference between anonymisation and pseudonymisation. Emphasis should be placed on explaining when a person could be reidentified, for what reason and by whom as people care about this and have a right to know. Furthermore, explaining such concepts honestly and with detail will build trust. The reluctance to do this for fear that people will say no, needs to be addressed properly. As noted people have been opting out of the GPDPR scheme in their millions because of the lack of clarity, transparency and detail coming from the government about the scheme and a lack of trust that the data won't be sold to third parties. We note that there are plans to provide more detail about the scheme, which we welcome. We look forward to seeing how the detailed complex issues are addressed and communicated to the public. Developing, and then maintaining trust is absolutely critical.

Overall approach

Overall, whilst we welcome the brave and bold intentions outlined in the draft strategy, balancing benefit with risk and harm will be critical. Ensuring data isn't being collected, shared and used without clearly defined purpose is an issue, as is the security and accuracy of commercial and clinical technology and the data collected and shared by use of API. In turn, these APIs and other related technologies must be properly secured so that opening up data to more sharing, does not in turn open it up to being easier to access by malicious actors.

Most importantly, we call on NHSX and the wider health and social care bodies, including the DHSC, to be clear and honest with people about what data is being discussed (is it for example, personal, non-personal, sensitive, clinical, location, anonymised, pseudonymised, re-identifiable etc) and what, why, where, how and with whom it will be shared. Data is a core part of life for patients and consumers, but not being straight with the facts is likely to cause new harms as a lack of trust deters people from engaging with or benefitting from data driven health services.

There is detail and subtle nuance in this complex and sensitive area. This is the detail that NHSX must understand in order to develop a strategy that can be successfully adopted. This detail is not possible to communicate via the survey that you have issued with this draft Strategy. We strongly advise NHSX and more broadly the DHSC, to engage in a more detailed and transparent way with patients and civil society; we agree “data saves lives”, so this point is critical.

We look forward to further engaging with you as the strategy develops.

For further information, please contact Renate Samson, Principal Policy Adviser, Which? via email at renate.samson@which.co.uk.