ico.
Information Commissioner's Office

Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
T. 0303 123 1113 F. 01625 524510
www.ico.org.uk

19 August 2021

Dear [redacted],

It was good to meet with you again on 29 July 2021 to discuss the Data Saves Lives: Reshaping health and social care with data draft strategy (the Data Strategy) in more detail. Following the discussion in that meeting, the comments attached at Annex A set out our formal response to the Data Strategy. Please note that these comments are based on our understanding of the initiative at this time. For clarity, please note that our engagement and commentary would not prevent the ICO from taking appropriate regulatory action in the future should this be required.

As per our comments in Annex A, the ICO would be a statutory partner in consultation where secondary legislation is used to enable proportionate data sharing, given the obligations for legislative consultation under Article 36(4) of the UK GDPR. Given the likely scale and breadth of these proposals, the ICO would need to be informed in a timely manner to ensure that there is sufficient opportunity for input before proposals are finalised.

The ICO welcomes initiatives within the strategy that will tackle challenges in using health and social care data. The pillars identified address important cultural, organisational, legal and technological challenges. As set out in our initial response to the draft Strategy the ICO supports an approach that will enable effective and innovative uses of data, backed by high standards of data protection.

The ICO recognises the benefits of appropriate data sharing in order to make improvements to patient care. Data protection law enables organisations to share data in a way that is targeted, fair, proportionate and secure. This is a key factor in securing public trust and confidence and we have seen this in the data-driven responses to the pandemic.

The ICO has also developed a range of guidance and services to support organisations innovating with data comply with data protection law. This includes the ICO sandbox, certification schemes, ICO data sharing code and guidance on AI. The ICO stands ready to engage with the sector as to how these initiatives can also engage with the proposals in the Data Strategy.

The ICO welcomes that there is a clear commitment to transparency throughout the document. However, there needs to be further clarity on how the public will be given greater control of their data in practice as well as greater transparency as to how their data will be used. Unless measures are clearly communicated, there is a risk that the public may not be properly informed or misunderstand their rights around the use of their data for research, as the General Practice Data for Planning and Research (GPDPR) debate has shown us. Effective and sustained transparency here will be of utmost importance, including evidence that it works in practice. As part of this sustained approach to transparency a long term plan for public engagement will also be vital.

As we highlighted in our meeting, data protection law sets out obligations through data protection by design which allow controllers for the data to demonstrate how they have built in measures which protect personal data from the earliest stages of the project and lay foundations for building public trust and confidence. The ICO is supportive of the use of Trusted Research Environments (TREs), subject to appropriate safeguards and governance, as a mechanism to deliver innovative uses of data alongside data protection by design.

We also emphasised the need for more prominence to be given in the Data Strategy to ensuring that data subjects can exercise their rights under data protection law, which is key to underpinning trust and confidence. We are open to discussing this further with you either in future meetings or separately.

As is our normal practice we plan on publishing our response.

We hope that our formal response provides helpful feedback as you finalise the data strategy and as agreed in the meeting last month, we will set up a follow up discussion in September.

Yours sincerely,

Ian Hulme
Director of Regulatory Assurance

Annex A

This is the ICO's formal response to the Data Saves Lives: Reshaping health and social care with data draft strategy (the Data Strategy). Following a review of the Data Strategy in detail we provide this feedback based upon our current understanding of the initiative.

The ICO recognises the benefits of appropriate data sharing and welcomes and supports initiatives which are backed by high standards of data protection. The response includes recommendations to ensure that a data protection by design approach is used. This will help to build in measures which allow controllers for the data to demonstrate how personal data has been protected from the outset as per their obligations set out in data protection law. We have also highlighted the need for transparency to ensure that the public are fully aware of how their data will be used and how they can exercise their rights.

The ICO are happy to continue to be involved in and support the development process. We would stress that this response does not form part of a formal consultation as per the requirements set out in Article 36(4) of the UK GDPR.

Please find below our detailed observations on each of the Chapters in the Data Strategy:

Chapter 1: Bringing people closer to their data

Harnessing data to improve patient and service user safety

We note that the current information governance (IG) website provides new guidance for staff on sharing data for patient care. This website should be developed in line with the Data Strategy so that it is consistent.

Significant commitment to AI is described here and elsewhere in the Data Strategy. The ICO has produced recent guidance on AI and data protection, including guidance produced in collaboration with the Alan Turing Institute on explaining decisions made using AI. Given the sensitive nature of the data, consideration should be given in the Data Strategy to the use of privacy enhancing technologies (PETs) as part of the AI workstreams. The ICO expects to produce guidance on PETs as well as anonymisation and pseudonymisation in 2021.

We note that effective communication and engagement with the public is needed around the use of their data for research. The recent controversy around the GPDPR programme has shown how important this is to building public trust and confidence.

Protections must be implemented and communicated when linking datasets to support this work to guard against scope creep or embedding disadvantage.

The Data Strategy needs to be clear about the role of private companies in the landscape of personal health records, both for adults and children. It is essential that organisations understand their data controller responsibilities and this must be clearly communicated to the public. The Data Strategy would also benefit by being clearer on previous statements by NHSD that controllership for personal health records (PHRs) would be shared between the health authority and the platform provider.

Bringing people closer to their data

Ensuring that everyone is able to access their own health and social care data is a positive step, and links directly to the right of access conferred by data protection law. The Data Strategy should however also consider how disclosure of information which should not be seen by the patient will be prevented, for example where a clinician considers that disclosure may cause them harm. Regard should also be given to how the right of access can be provided where individuals are lacking literacy (including digital literacy).

The ICO notes the relatively short timescale for the delivery of this commitment, and the Data Strategy should set out clearly how this will be achieved. It should also provide clarity on how the technology would work in practice as well as the technical and organisational measures to be implemented.

Giving people confidence

Commitments to increased transparency are welcome. We note the commitment to publish a ‘transparency statement’ explaining how health and care data will be used in 2022. Given that obligations around transparency are already present under data protection law it would be helpful for the Data Strategy to be clear on whether the intention is for it to go beyond the existing statutory requirements. If so, further details should be provided in the statement. Similarly, it may be that the commitment to allow citizens to identify who has had access to their data and the research this has informed is already covered by existing requirements under the right to be informed. It would be helpful for the Data

Strategy to be clear on this point. A layered approach to transparency is also important, to ensure the right information is provided to the public at the right point in their engagement with data use. Measuring the reach and effectiveness of transparency is also vital in such a universal area.

We note the commitment to an open-working approach across the sector to allow the public to easily find and identify data delivery work. The Data Strategy would benefit from being clearer on this commitment and how it would work in practice.

The ICO attends the Health and Care Information Governance Panel so we are familiar with its function and value. Utilising this panel to produce guidance, frameworks and standards to build public trust and confidence is therefore welcome.

Chapter 2: Giving health and care professionals the data they need to provide the best possible care

Simplifying information governance

The ICO welcomes the commitment to improve the resources available to staff, both through development of the Information Governance Portal as well as working with the National Data Guardian (NDG) to produce materials for staff. We look forward to continuing to support through our involvement in the working group.

Alignment of guidance at a national level will help to reduce regional disparities in information governance; there has often been variations between trusts and/or regions. There will be a challenge around aligning the NHS approach with other sharing partners in order to create the desired fluid sharing of data across the sector. NHSX should consider extending this guidance to other partners where appropriate.

We have published as a call for views the first chapter of our guidance on anonymisation and pseudonymisation which will provide useful advice when considering the rules around the use of data types, your input is welcomed. The ICO will be pleased to provide more detailed advice on this to ensure alignment.

The current information governance training for frontline staff appears to work well, though we note that more specific training for frontline staff would be advantageous. It is not clear whether the April 2022 deadline includes the development of new training products and rollout, or whether this is expected at a later date.

The intended simplification of the toolkits and language is noted. Whilst we welcome initiatives to make toolkits more accessible for users, care should be taken to ensure that messages are not diluted or diminished through simplification. Both aims should be able to sit alongside each other.

Creating a new duty to share

We recognise the importance of sharing data between the health and social care sectors, whilst also managing the risks this creates, and that using legislation to require sharing of anonymised data can address the gap that currently exists.

In order for this duty to be successful the ICO would highlight the importance of digital infrastructure to carry out this statutory duty. The Data Strategy should outline how this capability will be delivered as the work develops. It should also set out a commitment to ensuring the integrity of the system which will be critical in assuring data security and availability. The differences in maturity between social care and health care data collection systems is recognised elsewhere in the Data Strategy. The alignment and implementation of anonymisation standards will also be crucial. Audit and review of its operation, including the effectiveness of anonymisation, will also be important

Resources will need to be dedicated to staff training to ensure that any statutory duty to share is delivered compliantly. There is a risk that introducing this duty could be perceived as an administrative burden if the sector cannot be persuaded of the benefit.

Delivering shared records

The ICO does not have concerns in principle about the implementation of shared care records. However, it would be useful for the Data Strategy to include more detail on the difference between the basic and comprehensive shared care records referred to in this section, if indeed they are different.

Reducing the data collection burden

We note that the current focus of data alliance partnerships appears to be focussed on reducing administrative and clinical burden. You may wish to consider expanding the remit of such partnerships to include data protection considerations such as necessity and proportionality when considering whether data collection is appropriate.

Harnessing safe and effective innovation

Changes to digital care home projects must be fit for purpose. Some technology used in care homes (CareTech) involve surveillance which may be a disproportionate privacy intrusion on service users and visitors. Though the potential benefits of these technologies are noted, consideration must be given to how they may compromise privacy and what alternatives are available to address the problem.

Appropriate levels of security will be needed, given the sensitivity of the data to be processed. Within this, the resilience of the technology must be considered – for example, how the technology will work in areas of poor coverage or during an internet outage (and the impact such an outage may have on the individual).

Regulation of medical devices is still developing, and there are circumstances within the UK where 'wellbeing devices' do not receive the same level of scrutiny 'medical devices' do. There is a significant risk of devices being offered without awareness of whether they meet privacy or data protection standards. We consider that there is a need for a clear data protection standard for these devices.

Chapter 3: Supporting local and national decision makers with data

Integrating local care systems with a culture of interoperable by default

We would reiterate our earlier concern that the care sector may not have the necessary digital infrastructure to carry out this statutory duty at present. This is likely to be the case with both residential and domiciliary care providers, and separate solutions may be required to accommodate both systems.

Building analytical and data science capacity

No comments on this section.

Working in the open

The ICO welcomes the Data Strategy's commitment to transparency through the use of open-source code, recognising that doing so could help to address concerns about the use and impact of new technologies and innovation.

Sharing for wider purposes

The ICO would be a statutory partner in consultation where secondary legislation is used to enable proportionate data sharing, given the obligations for legislative consultation under Article 36(4) of the UK GDPR. Given the likely scale and breadth of these proposals, the ICO would need to be informed in a timely manner. This will ensure that there is sufficient opportunity for input.

The commitment to work closely with stakeholders and the public on these changes is welcome; we consider this will be a key factor in achieving the trust and confidence of the public and note that the NDG has had recent success in this area through its use of citizens' juries.

Collaborating with wider partners

The Data Strategy needs to explain how it intends to improve data linkage across government departments in more detail, including the issues that this would be addressing. Whilst there is the potential for benefit, this type of activity also has the potential to result in a risk to data subjects' rights and freedoms, and it will be crucial to take a data protection by design approach to mitigate risk to individuals and implement appropriate safeguards. Again, this is an area where engagement with the public about the use of their data and the resulting benefit will be an important factor in building trust and confidence.

Similarly, more detail is needed on the plans for public health agencies to draw on multiple data sources to gain new insights into the public's health. Reference is made to quicker access to high quality health intelligence. Further information should be provided in relation to this proposal. In particular, which data sources will be used, what type of data will be collected and what safeguards will be put in place to mitigate risk to individuals.

Chapter 4: Improving data for adult social care

Improving access to information for adult social care providers

We note that this Strategy acknowledges the difference in maturity between social care collection systems and health systems. The Strategy could be clearer however about the categories of data intended to be collected from 'client level', particularly as there may be some objection from the private sector about this data collection if it is not considered relevant.

The intention to provide a digital skills framework alongside training opportunities to improve data and digital literacy is a welcome step. However, this must be supported by private employers in the social care sector who will likely need to allow staff time and provide portable digital devices to enable this.

Integration of health and social care

Following on from our feedback on Chapter 3 of the Data Strategy, the ICO will be a consultee for any legislation conferring a duty to share personal data as per Article 36(4) of UK GDPR. At this stage, we would expect more detail on the categories of data to be collected, particularly from private organisations.

There should be an explanation of how the data framework for adult social care fits with the framework referred to elsewhere in the Data Strategy. This proposed framework appears to intersect with the requirement to maintain a record of processing activities set out in Article 30 of UK GDPR. Also, we have provided comments regarding CareTech and privacy under 'Harnessing safe and effective innovation', and these are relevant to the commitments made here.

Chapter 5: Empowering researchers with the data they need to develop life changing treatments, models of care and insights

The Data Strategy gives positive examples of how innovative uses of health data can embed data protection by design and default. This helps demonstrate that data protection legislation is not a barrier to proportionate sharing of personal data. The ICO aims to promote and encourage confident, responsible and lawful data sharing in the wider public interest. We support the development of trusted research environments as a way of implementing the requirements of UK GDPR Article 25.

Providing safe and secure data for analysis and research

The ICO recognises the value of partnerships between researchers and frontline analytical teams to improve skills and knowledge exchange, and to provide clarity on terminology. The latter will need to be supported by a communications campaign to encourage adoption.

Encouraging clinical research

When creating new at-scale data assets it will be important to consider how security can be assured, particularly through appropriate access control, to guard against misuse and security breaches. You should also consider implementing strategies to allow researchers to identify the most appropriate datasets for their project, for example, through metadata search or a sample data template. Doing so will help to protect the privacy of individuals within the dataset, as would the use of privacy enhancing technologies (PETs).

We would advise you to consider the potential for the international transfer of personal data when working with the G7 or other countries, and ensure that appropriate safeguards are in place.

Chapter 6: Helping colleagues develop the right technical infrastructure

Modernising our data architecture

We welcome the commitment to national standards for health and social care data. As mentioned above, the ICO is developing guidance on PETs, anonymisation and pseudonymisation which we expect to be published in 2021, which we believe will help inform your approach.

We would expect to see security explicitly added to the data architecture principles. The Data Strategy would benefit from being clearer about the technical and organisational security measures intended for adoption to secure the Application Programming Interfaces (APIs) which will supply data to the NHS Account, and whether any PETs will be considered here. More detail on security would also be useful on the roadmap for core services using cloud technology.

The Strategy would benefit from clarifying what is meant by improving onboarding to increase the uptake of national services and products (such as the NHS number).

Further detail is also required on the commitment to increase the amount of APIs available on the national healthcare gateway by August 2021. In particular, the Strategy would be improved if the benefit of introducing these APIs were articulated.

Information Asset Owner models are well established and give clear ownership. A more centralised model may bring conflict with this. Responsibility and ownership for information assets should be considered from the outset. Clarity on any changes with the development of data infrastructure services to support interoperability would help us to consider the potential data protection implications of this work.

Promoting and developing new data and technical standards

The UK GDPR contains some broad data quality standards. For example, the accuracy principle requires that data be accurate and up to date, while the data minimisation principle requires data be adequate, relevant and limited to what is necessary. It appears that the development of data standards would be compatible with these principles. If legislation is used to achieve this, the ICO would need to be consulted under UK GDPR article 36(4).

The development of core, UK-wide Fast Healthcare Interoperability Resources could bring some challenges, for example data accuracy and quality issues have previously been seen in national patient databases (eg the Spine). NHSX should learn lessons from previous experience, eg will a data cleansing exercise be required? The risk of excessive collection and/or retention of personal data should also be considered.

We would encourage that how the adoption and tracking of standards will be monitored is outlined in the strategy, including how compliance will be monitored and who would be responsible for that monitoring.

Staying ahead of the evolving cyber risk

This section could be improved by considering protection of services separately from protection of information. The two risks are somewhat different, which isn't drawn out in this section. Reference to confidentiality, integrity and availability would also be appropriate.

As the intention is to shift from siloed environments to more centralised, accessible data, the Strategy should carefully consider role and/or attribute based access controls as well as the minimisation of accessible data. Control and review of appropriate data views and schemes based on specific requirements and purposes should also be considered to avoid access to excessive data.

Consideration should be given to the risk of single points of failure and attendant backup and security measures.

At this stage the specification is at an understandably high level and abstract, referencing 'what' they wish to achieve. As work progresses the ICO would anticipate the addition of detail around cybersecurity arrangements, specifically around 'how' the objectives will be achieved. Specific domains that will require consideration include:

- Appropriate information security controls including internal and network edge firewalls, network security management, secure configuration practises, appropriate management of removable media and online file repositories.
- Highly effective access control with a well thought out role or attribute based access control model along with industry standard authentication and two factor authentication methods. There should be more stringent controls around allocation of privileged user rights in a centralised model bearing in mind the significant access to data that privileged users will have.
- There should be an effective log retention management and analysis process.
- There must be appropriate protection against malware, vulnerabilities and other forms of cyber security attack with regular penetration testing and/or other forms of auditing.
- There should be appropriate security controls around software development and procurement including code quality review, anonymisation of personal data in development environments on the robust development test and release model.
- There should be a training programme in place to ensure understanding and compliance with data protection legislation and industry standards backed up by an appropriate training needs analysis and this should be reinforced with appropriate awareness raising campaigns.

Separating the data layer

The Strategy should be clearer on timescales for this commitment. It would also benefit from further detail on the safeguards in place to ensure that providers delete personal data as contracts end. Security measures to protect the data layer will be crucial, particularly where innovation is incorporated. Opening up access to live patient data for the purposes of application development raises significant data protection and information security risks and we would expect stringent, effective and robust controls around any such access.

Populating the data layer with diagnostic and medicines data derived from COVID initiatives could link potentially sensitive information with patient data. The effectiveness of technical security measures will be critical, as will a Data Protection Impact Assessment (DPIA).

The Strategy could also be clearer on how standardised API access to shared care records will alter current practice – will this result in increased access to patient records?

Chapter 7: Helping developers and innovators to improve health and care

Driving interoperability for innovation

The ICO welcomes commitments to improve transparency outlined in this section, however the Strategy would benefit from more detail around deadlines.

Clear and understandable AI regulation

Significant commitment to AI is described. The ICO has produced recent guidance on AI and data protection, including guidance produced in collaboration with the Alan Turing Institute on explaining decisions made using AI. We would be keen to engage with the development of national standards and strategies to assist with incorporating data protection by design.

The use of PETs and synthetic data will be important considerations when developing standards and strategies, as well as when working with regulators to ensure fitness for purpose. We again consider that our upcoming guidance in this area will be of assistance to you. It will be important for the ICO and NHSX to work closely on developing an approach for independently validating AI technologies for screening, and we note the tight timescale for intended delivery.

Supporting innovators to work with health and care organisations

The ICO would be pleased to share our experience in this area. We offer a Regulatory Sandbox to innovators, as well as techsprints and our Innovation team's Grants programme.