Upholding information rights

Queen Elizabeth House, Sibbald Walk,
Edinburgh, EH8 8FT
T. 0303 123 1115 E. scotland@ico.org.uk

Gillian Martin MSP
Health, Social Care and Sport Committee
The Scottish Parliament
Edinburgh
EH99 1SP

By email only: hscs.committee@parliament.scot

12 December 2022

Dear Gillian,

Follow-up to attendance at HSCS Committee, 22 November 2022

Thank you for inviting me to provide evidence to the Committee on the above bill. Please find my response to your further questions below.

Implementation risks

- *Do you recognise particular concerns about the impact on service users during the period of transition to new data systems and new approaches to information sharing as part of the Bill's implementation? What are those concerns and how might they be addressed?*

The Bill provides little detail on these new systems and the specifics of future information sharing. I can therefore only comment generally on the risks that would be present in any significant change of this nature. The health and care systems together process a high volume of special category data relating to approximately 5.5 million individuals. Any significant changes to this processing therefore necessarily carries high risks. Significant care must therefore be taken at the design, development and delivery stage to ensure that high standards of data protection are met and in particular that the legal obligation of data protection by design and default is complied with.

To address these risks it will be critical that privacy friendly system design solutions are selected and that the system design allows for, and supports:

- compliance with the data protection principles (e,g through careful design of security and access controls, retention and weeding functions, logging and purpose limitation features);
- adherence to the ICO Data Sharing Code of practice;

Queen Elizabeth House, Sibbald Walk,
Edinburgh, EH8 8FT
T. 0303 123 1115 E. scotland@ico.org.uk

- conformity (where applicable) to the ICO Children's Code and design guidance;
- access and delivery of individual's data protection rights.

Completion of a Data Protection Impact Assessment (DPIA) prior to implementation is a legal obligation where processing is likely to result in a high risk to individual's rights and freedoms.

The DPIA process should begin at an early stage and should involve:

- developing a clear understanding of the intended data flows and roles and responsibilities of all relevant bodies at an early stage;
- consultation with both service users and controllers;
- a comprehensive risk assessment and identification of mitigations and safeguards to reduce risks to individuals;
- consultation with relevant Data Protection Officers and, where appropriate the ICO;
- the development of Data Sharing Agreements where appropriate;
- ongoing review and monitoring of risks.

Ownership and control of data

- *To what extent do you believe Part 2 of the Bill as currently drafted reflects a human rights-based approach? What changes might be needed to ensure individuals' human rights are respected and protected in the implementation of this Part of the Bill?*

The ICO has no concerns about the current drafting in relation to data protection rights however I would like to stress that any concerns would only become evident in the more detailed regulations.

Scottish Ministers are obliged (under Article 36 (4) UK GDPR) to consult with the ICO when preparing any legislative proposals that involve the processing of personal data and we would expect to engage on the detailed proposals at that stage. Given the significance of the reforms we expect the formal consultation with us on the secondary legislation to commence at least 12 weeks prior to the final proposals being laid in parliament (as set out in DCMS guidance).

- *What role would you expect Care Boards and/or Ministers to fulfil in relation to the control of data? Is this sufficiently clear in the Bill?*

It is not possible to provide any detailed comments on this at this stage as controllership will be dependent upon roles and responsibilities outlined within

Upholding information rights
Queen Elizabeth House, Sibbald Walk,
Edinburgh, EH8 8FT
T. 0303 123 1115 E. scotland@ico.org.uk

secondary legislation. Officials should discuss these matters with us prior to the drafting of regulations and thus ahead of the formal consultation under Art 36(4) of the UK GDPR

- *The Committee has heard evidence of an appetite among people who use services to own their own data, which Mydex CIC discussed in some detail in their written evidence to the Committee. During the meeting, you raised a range of issues about this concerning regulation, high level data capture and data protection. The Committee would be grateful if you could provide more detail about the nature of these concerns, whether there is an opportunity to create an abbreviated care record that an individual could use/own to prevent the repetition and retraumatisation people currently experience when seeing different professionals or whether the shared care record scheme outlined in the Bill would be sufficient to address this issue?*

There was some discussion at the evidence session as to whether consent should be sought before any information is shared. Our concern is that, given the power imbalance that exists between health and care providers and patients, it is very difficult for public authorities to gain valid consent for data sharing under data protection law. This is particularly the case in situations where there is a safeguarding concern or in an emergency where the individual has either not provided consent or is unable to provide consent to share data but yet it is necessary to do so to protect against serious harm or risk to life. There may also be situations where sharing certain information with a patient may present a serious risk of harm and exemptions within data protection law recognise this.

Given the difficulties with obtaining valid consent outlined above our recommendation is that the focus should be on fair and transparent processing. This means ensuring that individuals receive clear and accessible transparency information about how and why their data will be processed and how they can access their rights and raise concerns. It also means ensuring that their data is not processed in a way that they would not reasonably expect or which would cause an unjust adverse impact. To comply with the fairness principle controllers should seek to understand the views, reasonable expectations, experiences and concerns of patients and service users and work with them to identify and mitigate/safeguard against likely harms and impacts on rights and freedoms. The views of the individual should be sought and considered when making decisions about which data should be shared with which controller for which purpose.

A more unified health and care record has the potential to deliver benefits to patient care and to prevent re-traumatisation when individuals have to provide the same information to different professionals. Implementing high data

Upholding information rights

Queen Elizabeth House, Sibbald Walk,
Edinburgh, EH8 8FT
T. 0303 123 1115 E. scotland@ico.org.uk

protection standards and complying with the fair and transparent principles will help ensure public trust and prevent harms.

Monitoring and evaluation

- *Are there specific gaps in currently available health and social care data which will need to be addressed to enable effective monitoring and evaluation of the proposed National Care Service?*

We cannot comment on this.

- *Are you able to address in further detail the interplay between a scheme that would allow for sharing of a care record and the gathering and collation of health and care information to assist with the planning of services, at a local and national level?*

We do not have comments to make on this other than to note that we can see that a unified health and care record and consistent data standards could offer benefits in this regard and that and that data protection law provides a framework to allow this processing to be carried out fairly and securely.

I hope the answers above are helpful. Should you need any further detail please do not hesitate to get in touch.

Yours sincerely

Ken Macdonald
Head of ICO Regions

Information Commissioner's Office (Head Office)
Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
T. 0303 123 1113