## Introduction

1. Data protection law provides an effective framework for processing personal data, enabling innovation but also protecting people. Compliance with data protection promotes greater trust and confidence by the public.
2. The Commissioner supports the government's ambition to reform the health service to make it fit for the future. In particular, the Commissioner supports the drive to harness the potential offered by digitalisation and AI technology to drive improvements and innovation in patient care and economic growth.
3. Where we see that the appropriate steps have been taken to safeguard information, the ICO can play a role in providing reassurance to the public, particularly in cases where patient centric approaches are used to improve patient outcomes.

## About the Information Commissioner

4. The Information Commissioner has responsibility for promoting and enforcing data protection and information rights. This includes responsibilities under the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA), the Freedom of Information Act 2000 (FOIA), the Network and Information Systems Regulations 2018 (NIS), and the Privacy and Electronic Communications Regulations 2003 (PECR).
5. The Information Commissioner is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
6. The Commissioner provides guidance and support to individuals and organisations, aimed at helping organisations to comply, and takes appropriate action where the law is broken.

## ICO collaboration with the health and care system

7. The ICO provides data protection advice to the health and care system through its engagement with leading stakeholders from across the 'health and care' and 'life sciences' sectors. This includes regular engagement with DHSC, NHS England (NHSE) as well as the DHSC's 'joint unit' with NHSE, NHS bodies and the National Data Guardian.
8. Through our attendance at the joint unit led 'Health and Care IG Policy Group' and associated working groups, the ICO provides advice to leading organisations developing information governance and data protection guidance.
9. During the Covid-19 pandemic, the ICO was responsible for providing advice to Government and NHS bodies on data protection issues relating to key programmes including the Covid19 Contact Tracing app - Test and Trace, and vaccine delivery

initiatives. During this period, we made clear that data protection legislation allowed for the use of data for these purposes where there is a clear public interest.

10. We provide advice on key strategic programmes in health and care such as the Federated Data Platform, attending the programme's Check and Challenge and Information Governance advisory groups run by NHSE to scrutinise and challenge the programme to achieve its goal of protecting patient data, keeping it secure and only using it for authorised purposes.

**The 10-year plan**

11. The ICO welcomes the development of the 10-year plan and the opportunity to contribute to this consultation.
12. Whilst the consultation questions primarily concern ideas for improving the provision of health and care services (which sit outside the ICO's remit), there are aspects of the consultation where data protection needs to be at the centre of thinking. Incorporating 'privacy by design' into the Government's ambitious programmes would give that patient centric approach and act as a touchstone for maintaining trust.
13. We intend to address these points and provide broader comments on data protection considerations that can facilitate enabling better use of data to support future proposals included as part of the 10-year plan.

**Consultation Question 1 - What does your organisation want to see included in the 10 Year Health Plan and why?**

14. The ICO expects Government to take a privacy by design approach for a data use proposed within the 10-year plan and ensure that the following challenges are resolved in ways that build trust and confidence;

**Transparency**

**15. The ICO would like the 10-year plan to consider transparency holistically, to ensure transparency information is delivered effectively across the whole health and care system. Deciding who should be responsible for delivering it across different points in the health and care system will ensure that this is done effectively and in a consistent manner.**

16. Transparency is the mechanism by which people find out about how their information is used. Transparency is therefore fundamental to data protection individual rights - people can only exercise their rights if they know when their information is being processed, for what reason and which rights may apply.

17. The ICO's research into Public Attitudes to Information Rights suggests that a significant part of the population are not aware of their data protection rights. Our Data Lives research also suggests that the public aren't always aware of the risks associated with their data being used. It is, therefore, important to be transparent about how data is being used to ensure that people who are not aware of their rights are protected and informed about what is happening with their data.
18. Transparency is also a vital tool for building trust and confidence amongst the public for how their information is used. By being transparent people will have more trust and confidence in the programme.
19. Patient engagement processes can help identify how the public feel about certain forms of information use as well as inform how transparency information is developed and delivered.
20. The ICO has recently published guidance to help organisations that process health and social care information understand our expectations about transparency and how to comply with the law. The guidance was produced in consultation with stakeholders from across the health and social care sector.

**Information Rights**

**Right of Access**

**21. The 10-year plan should consider the data protection risks associated with providing increased levels of access to clinical information.**

22. The right of access is a fundamental data protection right that ensures people have access to information for a variety of reasons, including making informed decisions about their own health care. Recent developments in the health and social care sector relating to information access include making patient medical records automatically available through the NHS App and other online services.
23. The ICO is supportive of plans that further facilitate the public's access to their health and care data in this way, as long as the appropriate safeguards are in place.
24. Risks and challenges associated with increasing access include controllership issues (see below) that result from the fragmented nature of health and care providers, as well as ensuring strong safeguards remain in place to protect individuals in cases where providing access is likely to result in serious harm.

**Right to Object**

**25. Government should ensure that people understand and are able to easily exercise their right to object.**

26. The right to object to processing under UK GDPR is distinct from the local and national patient opt-out rights (ie National Data Opt-out).

27. Managing preferences, opt-outs and objections in clinical settings remains complex, with competing definitions and applications. Whilst these choices offer assurance to the public on how their information is used, the landscape remains confusing for the public to understand and take effective action when required.
28. The 10-year plan should consider and set out how an individual's right to object to their data being processed can be exercised in circumstances where controllers do not have compelling legitimate grounds.

**Use of Technology (including AI and Automated Decision Making )**

29. **The ICO supports the innovative use of technology to improve patient outcomes, as well as to promote economic growth. However, the use of such technology needs to be done in a transparent manner and must uphold individual rights. The ICO would like to engage with the NHSE at an early stage when innovative technologies are being developed to ensure that data protection is implemented by design and by default.**
30. The ICO recognises the potential benefits of using innovative technologies when processing health and care information and a key aspect of our ICO 25 strategy is to empower responsible innovation. The ICO would be supportive of any changes that improved the pathways for innovators and researchers to access data as long as appropriate safeguards are in place.
31. However, the introduction of innovative technologies must also ensure the rights and freedoms of individuals are upheld. In particular, the use of these technologies should be fair, lawful and transparent, in accordance with data protection legislation. The public should be informed at an early stage of the development of new innovative technologies that may affect their data to enable clear transparency.
32. The application of new technologies, including artificial intelligence (AI), must also comply with the rules around automated decision-making and should be thoroughly tested to ensure that decisions are accurate and that the risk of any inherent bias is mitigated. You should also be transparent about the use of such new technologies and inform individuals prior to any data being processed in this way.
33. Where the 10-year plan introduces proposals that are underpinned by such technology, the security of the data, as well as the rights and freedoms of the data subjects, must be upheld. The ICO would like to receive assurances at an early stage that this is the case when new or novel use of technologies are being considered.
34. The UK GDPR requires that a data protection impact assessment must be conducted if the processing is likely to result in a high risk to the rights and freedoms of individuals, particularly when using new technologies.

35. The personal information involved in the use of new technologies must remain secure. This can be achieved using encryption, pseudonymisation, or other methods.
36. Cyber security is becoming increasingly important with the increased digitisation of healthcare. It is essential that health organisations ensure appropriate security and cyber resilience, updating systems, policies and procedures at pace with new technology developments.
37. Privacy Enhancing Technologies (PETs) have allowed for increased levels of privacy friendly data sharing, particularly for secondary purposes such as public health management and clinical research. The ICO has published a range of guidance on PETs, and a further chapter relating to research will be published for consultation in 2025 as part of our Anonymisation guidance.
38. The ICO remains supportive of the NHS's use of secure data environments (SDEs) to provide researchers with access to high quality information to improve outcomes for the public. SDEs may be used to assist with the security of personal information, however other aspects of the legislation still need to be considered. These include minimising the amount of data being used to what is necessary.

**Comments on proposals for a single health record**

39. The ICO is aware of plans to introduce a mechanism to link disparate forms of patient medical records (ie, GP record and Hospital trust) together in a single patient record.
**40. The ICO expect Government to address the following data protection challenges when developing the single health record;**

**Controllership**

41. Separate clinical and data protection responsibilities should be agreed upon and well understood before sharing information in new ways. As the recent Sudlow report notes, "Some GPs have concerns about inadvertently breaching laws that protect the confidentiality and privacy of patient data."
42. Friction between controllers arises where clinical and governance responsibilities are not clear, and this can present as a data protection issue where this may not necessarily be the case (such as other contractual obligations or resources).

**Access control & monitoring**

43. The public should be assured about the existing controls already in place that limit access to confidential information to those that need it, which can be achieved

through increased levels of transparency. New measures introduced as part of the single record programme could provide further assurance.

**ICO Support**

44. We hope our response to this consultation is helpful and the ICO stands ready to provide advice and regulatory oversight to new initiatives linked to the 10-year plan, through its ongoing engagement with DHSC and leading NHS organisations.