Response of the Information Commissioner's Office to the Department of Health and Social Care's call for evidence on 'Equity in Medical Devices'

About the Information Commissioner's Office

1. The Information Commissioner's Office (ICO) has responsibility for promoting and enforcing the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA18), the Freedom of Information Act 2000 (FOIA), the Privacy and Electronic Regulations 2003 (PECR), the Network and Information Systems Regulations 2018 (NIS) and the Environmental Information Regulations 2004 (EIR).

2. The ICO is independent from government and upholds information rights in the public interest, promoting transparency and openness by public bodies and organisations and data privacy for individuals. It does this by providing guidance to individuals and organisations, solving problems where it can, and taking appropriate action where the law is broken.

Introduction

3. The ICO welcomes the opportunity to respond to this independent review commissioned by the Department of Health and Social Care (DHSC) to report to the Medicines and Healthcare products Regulatory Agency (MHRA) for evidence on equity in medical devices (including AI-enabled medical devices).

4. Ensuring technologies treat people and their information fairly, as well as identifying and addressing the risk of technologies adversely impacting vulnerable groups are aims the ICO shares. Fairness is one of data protection's foundational principles and through its ICO25 strategic plan the ICO has committed to safeguarding the most vulnerable.[1]

[1] ICO25 - Empowering you through information

5. AI is a strategic priority for the ICO. ICO25 highlights our plans in this area, including work to tackle urgent and complex issues such as AI-driven discrimination.[2] This builds on our existing work on AI, including:

- our landmark Guidance on AI and Data Protection[3];
- our accompanying AI and Data Protection risk toolkit[4] (recently shortlisted in the Global Privacy Assembly's Global Privacy and Data Protection Awards[5]);
- our supplementary guidance on Explaining Decisions Made with AI co-badged with the Alan Turing Institute[6];
- our support for AI innovators through our Regulatory Sandbox and Innovation Hub[7];
- our contribution to standard-setting initiatives as a member of the AI Committee of the British Standard Institution (BSI); and
- our supervision of organisations using AI, including through both proactive audits and investigations.

We continue to track developments in AI to ensure that our positions reflect the latest technological opportunities and risks.[8] We therefore stand ready to work with DHSC and MHRA to assess opportunities for interventions that will deliver clear benefits for the public.

6. Data protection law already plays a critical role in addressing the concerns highlighted in the call for evidence. Developers of medical devices have existing responsibilities under data protection legislation (including the UK GDPR and DPA18) to ensure that they are creating and deploying medical devices which process people's personal data fairly and do not lead to unjustified adverse effects. Whilst the primary aim of this publication is to seek evidence of issues in the design, development, and use of medical devices, as well as evidence of potential solutions to these, the role that data protection plays in safeguarding the public when its personal data is

[2] The ICO will soon update the fairness component of the existing Guidance on AI and Data Protection with the aim of assisting organisations tackle such issues.
[3] https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-ai-and-data-protection
[4] https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-ai-and-data-protection/ai-and-data-protection-risk-toolkit
[5] https://globalprivacyassembly.org/news-events/gpa-awards/
[6] https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/explaining-decisions-made-with-artificial-intelligence/
[7] https://ico.org.uk/about-the-ico/what-we-do/ico-innovation-services
[8] You can read more about ICO's work on AI here: https://ico.org.uk/about-the-ico/what-we-do/our-work-on-artificial-intelligence

processed, should not be forgotten as proposals for potential solutions are developed.

The ICO's role in regulating medical devices

7. The ICO plays a critical role in ensuring medical devices process people's personal data fairly and that processing does not result in unjustified adverse outcomes that would be deemed unfair.

8. Often the development and use of medical devices is inextricably linked to the processing of personal data. This means that the controller for the data processing undertaken on the medical device is accountable for ensuring that any processing of personal is carried out in compliance with data protection and they can demonstrate it. Where the developer of a medical device is a different entity to the one who deploys it, the accountability of different entities under data protection requires additional attention, identifying respective processor, controller, or joint controller responsibilities. All entities have a role to play in ensuring fairness and equitable outcomes.

9. Below, we set out elements and provisions of data protection that play a role in mitigating harms associated with medical devices and inequitable outcomes.

Fairness

10. The call for evidence focuses on ensuring equitable outcomes for people of different ethnicity or other social or demographic characteristics. In this context, DHSC and MHRA should note the existing fairness requirements of UK GDPR. Whilst there are overlaps, 'fairness' in a data protection context is a distinct concept to equity. Equity focuses on outcomes, ensuring that they are proportionate, whereas fairness encompasses both how personal data is processed and what the outcomes are for people.

11. A key principle of the UK GDPR is that personal data should be processed lawfully, fairly and in a transparent manner. To process personal data fairly means to process it in a way that the person reasonably expects and that any adverse effects for that person – if any – are justified. Developers and deployers of medical devices that process personal data are required to do so fairly.[9]

[9] We use the terms 'developers' and 'deployers' to distinguish broadly the two types of players in a medical device supply chain. A 'deployer' could be a clinical provider or a care provider. In data protection, a 'deployer' is most likely going to be a controller, and the 'developer' may be a

12. In order to assess whether personal data is being processed fairly, the controller for the data processing undertaken on the medical device must consider more generally how it affects the interests of the people concerned – as a group and individually. If they have obtained and used the information fairly in relation to most of the people it relates to but unfairly in relation to one individual, there will still be a breach of data protection's fairness principle.

13. Some medical devices generate solely automated decisions (ie without human oversight), with effects that are as significant in nature as a legal decision. In this case, UK GDPR requires controllers to implement appropriate technical and organisational measures that mitigate the potential risks of discriminatory effects on people based on their racial and ethnic origin, genetic or health status or sexual orientation or other special category data. This is likely to apply particularly where AI-enabled medical devices are being used for diagnosis or healthcare decision-making.

Transparency

14. The transparency principle is closely linked (but separate) to the fairness principle. It ensures that people whose personal data is being used in the development or deployment of a medical device are aware of how their data is being used and whether it is being used in a way that they reasonably expect.

15. UK GDPR requires organisations that process personal data, including medical device developers and deployers, to provide people with clear information about the personal data collected, what they do with it, who it is shared with, and how individuals can exercise their data protection rights in relation to it.

16. If done correctly, transparency can bring about significant benefits, including improving public trust and confidence. The controller for the data processing on the medical device needs to publish a publicly accessible privacy notice that provides clear information to people about how their information is being processed and how they can exercise their rights. This includes where they are processing personal data to assess equitability of medical devices.

---

processor, or in some circumstances, a joint controller. The 'developer' is likely going to be a controller for any processing of personal data during the design and testing phase of a medical device.

17. The risk of opaque processing can be exacerbated where AI models are used in medical devices. Some AI models are 'black boxes,' i.e. they are difficult or impossible to interpret or explain outcomes produced from the medical device. This may also make the processing unfair where people have a reasonable expectation to know how a decision has been made about them. The controller for the data processing undertaken on the medical device should think carefully about the risks and potential impacts of using a 'black box' AI system. They could consider using supplementary interpretability tools to improve the explainability of their device if they believe that their use of a 'black box' AI system is appropriate within the medical device.

Lawfulness

18. When assessing equity in a medical device, the controller for the data processing undertaken on the medical device will need to have an appropriate lawful basis to process the data for that purpose. Additionally, they may need a further condition if the assessment involves processing special category data.

Automated decision-making

19. Data protection law has additional provisions for solely automated decision-making with legal or similarly significant effects. Article 22 of the UK GDPR says that people have the right not to be subject to this type of processing unless certain conditions are in place. These include the right to a meaningful human review.

20. As AI-enabled medical devices become more advanced, it becomes more probable that their use will fall under Article 22. Therefore, the deployer of these devices needs to consider the conditions set out in the provisions.

Data protection by design and default

21. Additionally, data protection by design and by default is a requirement of data protection. This means medical device developers must integrate data protection into their processing activities and business practices, from the design stage right through the lifecycle, including when decommissioning or recalling a medical device. By taking a data protection by design and default approach, medical device developers can increase the likelihood of their device delivering equitable outcomes. However, the controller for the data processing undertaken on the medical device will still

need to regularly assess the outcomes to ensure the processing remains fair, through regular monitoring and risk assessments.

22. In many cases, the use of a medical device is likely to result in a high risk for individuals. In such a case the controller for the data processing undertaken on the medical device should carry out a data protection impact assessment (DPIA) to identify and minimise the risks. A DPIA could include, for example, the risks of using personal data as part of the development or deployment of the medical device and the measures to mitigate it. A DPIA must be carried out before any processing of personal data. The controller should see DPIAs as living documents and should regularly update them.

Enabling innovation in medical devices

23. The ICO's Innovation department is committed to enabling innovation in medical devices. As part of our commitment, we are:

- Working in partnership with Connected Places Catapult in their Homes for Healthy Ageing programme. Our Innovation Hub mentors innovators to imbed data protection by design into their solutions to help older people age at home, assisted by technology.
- Collaborating with the National Data Guardian and MHRA to support the compliant development of health apps and wearables by developing a multi-agency handbook for innovators.
- Working with The National Institute for Health and Care Excellence-led Multi Agency Advice Service to create a sole source of information and guidance for developers and adopters of AI in health.
- Supporting innovators in our Regulatory Sandbox to create products and services which use personal data in innovative and safe ways.

We will continue to support innovation in medical devices by collaborating with key stakeholders in this space, whilst promoting a high standard in handling people's personal data.

Conclusion

24. The ICO supports the Government's vision to make medical devices equally effective and safe for everyone, regardless of their ethnicity or other social or demographic characteristics, such as socio-economic status. This call for evidence will provide a solid base for

what work needs to be done to make medical devices more equitable.

25. In seeking to tackle the challenge of equity in medical devices, close cooperation with the ICO, MHRA, Care Quality Commission (CQC) and the Equalities and Human Rights Commission (EHRC) will be required to ensure alignment and consistency across regimes and delivery of coherent outcomes. The ICO benefits from a close and effective relationship with these bodies, and the government should make full use of this collaborative arrangement as it establishes the role those existing regulators must play in this space.

26. We agree that the controller for the data processing undertaken on the medical device must assess the equitability of their medical devices. We also want to emphasise that most medical device developers and providers will be subject to the requirements set out in the UK data protection framework. This will include ensuring that any processing of personal data is fair. Whilst data protection's fairness principle and the concept of equitable outcomes are similar, they are distinct and therefore, there needs to be attention to both.

27. We look forward to seeing a summary of the results to this call for evidence. We also are open to further engagement with DHSC and MHRA on this issue.