Technology and innovation in the NHS

Information Commissioner's Office

1. The Information Commissioner has responsibility for promoting and enforcing the Data Protection Act 1998 (the DPA) and the Privacy and Electronic Communications Regulations 2003 (PECR), as well as the Freedom of Information Act 2000 (FOIA), the Environmental Information Regulations 2004 (EIR) which apply to reserved matters in Scotland. She is independent of government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations, solving problems where she can, and taking appropriate action where the law is broken.

2. From 25 May 2018, the General Data Protection Regulation (the GDPR) will come into force as the UK's new data protection legislation, supplemented by a Data Protection Bill that is to be introduced to the UK Parliament. The GDPR will raise the standard of data protection law and require greater accountability of organisations and enhances the rights of individuals.

3. The Commissioner welcomes the opportunity to respond to the Health and Sport Committee's call for views on 'Technology and innovation in the NHS', including the Scottish Government's draft vision for digital health and social care 2017-2022. Given the timescale involved, the Commissioner provides her comments in the context of GDPR being the law for most of this period. The Scottish Government and the NHS should plan ahead on this basis.

4. The Commissioner believes that public trust and confidence in how their personal data is used is essential to trust in new technology and other innovative practices. In any event, data protection law must be complied with and individuals' rights upheld.

Fairness, lawfulness and transparency

5. The Government's draft vision anticipates the use of personal data of the people using health and social care services. The use of that personal data must be both fair and lawful in order to comply with data protection law.

6. People have a right to know what information an organisation holds about them and the purposes for which it is being used. While this will often be apparent to the individual where the purpose is to provide them with care, there are other purposes which may be less obvious, such as medical research.

7. Indeed, the management of healthcare and the allocation of scarce resources, means that the use of patient data has never been more valuable to evidence-based decision making for the provision of health and social care. It is imperative that patients are fully aware of the different uses to which their data might be put and given the opportunity to

object when relying on consent or understand why it is deemed necessary and consent is not appropriate.

8. As well as informing the individual, the NHS must ensure that it has a legal basis under articles 6 and 9 of the GDPR for each of the different ways it uses patient health information. It is vital that any new practices identify that basis at the outset in order to ensure that it is lawful.

Data protection by design and default

9. The GDPR will require organisations to adopt a data protection by design and default approach to their use of personal data. This will require a data protection impact assessment (DPIA) to be carried out in certain circumstances. This includes where the processing of personal data by new technologies is likely to result in a high risk to individual's rights and freedoms. A DPIA is similar to the Privacy Impact Assessments (PIA) that the Commissioner has promoted for many years.[1]

10. Europe's data protection authorities (as the Article 29 Working Party) have adopted guidelines in respect of the GDPR on whether processing is likely to result in a high risk.[2] The guidelines recommend that where at least two of the ten listed criteria are involved in any new processing activity, the organisation should conduct a DPIA. These criteria include the use of sensitive personal data, including patient health information, and innovative use or application of technological or organisational solutions.

11. The Commissioner investigated the provision by the Royal Free London NHS Foundation Trust of 1.6 million patient records to Google DeepMind as part of a clinical safety initiative. She found that a PIA had been conducted by the Royal Free London but only after the records had been handed over. Had it been conducted earlier, the data protection risks may have been identified and mitigated to protect patients' rights.

Security of patient data

12. The GDPR requires that an appropriate level of security is applied to personal data, taking into account the nature, scope and context of the data, the state of technology, the risks to individuals of a compromise of that personal data and the costs of implementation.

13. Recent high-profile cyber-attacks, including the WannaCry ransomware attach of May 2017, have demonstrated the real impact that insecure software can have on patients. The expectation that patient information will be captured digitally means that the NHS and others must ensure they build strong defences into electronic systems and keep up to date with emerging threats and take as much preventative action as possible.

---

[1] Privacy Impact Assessment code of practice, Information Commissioner's Office, 25 February 2014 https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

[2] Guidelines on Data Protection Impact Assessment (DPIA), Article 29 Data Protection Working Party, 4 April 2017 http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

14. The ICO issued Gloucester City Council with a civil monetary penalty of £100,000[3] for failing to implement a software patch that could have prevented personal data being exposed as a result of the 'Heartbleed' virus.

15. It is not only electronic security that needs to be considered. As new systems and ways of working are introduced, it is equally important that NHS boards have appropriate policies and procedures in place to govern the use of personal data. They must also ensure that staff are aware and trained in these policies and procedures to avoid inadvertent breaches of personal data.

16. Collaborative working can also be a way of innovating. This could be with partner agencies, or engaging third-party services. Partnership working must be fair, lawful and transparent to the individual as described above. Where the NHS engages a contractor (data processor) to provide a service on its behalf, including the processing of personal data, article 28 of the GDPR requires there to be a written contract that sets out the parameters of the processing, the physical, technical and organisational security measures that must be in place and any other instructions necessary to set out what the data processor can and cannot do.

17. The concept of data protection by default and design means that finding a suitable data processor who can give robust guarantees about how they will process data on behalf of the NHS board should be established at the procurement stage.

Accessibility and sharing of the patient record

18. With the integration of health and social care and the increasing imperative for the sharing of sensitive personal data both within and between organisations, access to the patient record and the data therein has never been more in demand.

19. Access by third parties to the patient record must be on a need-to-know basis with each request justifying why that access is necessary. Consideration must be given as to whether the patient is to be contacted at each such request to provide their consent or whether one of the other conditions for processing is to be relied on.

20. Any access should be appropriate and proportionate for the specific purposes and patients must be made aware of who might be accessing their record or with whom their data might be shared. This will be particularly relevant for compliance with the GDPR from next year.

21. The ICO is aware of more prolific access to the patient record being given to third parties such as Community Pharmacists and in some locations this has been mooted to extend such access to opticians and other such health care professionals. For any such proposal, a full Data Privacy Impact Assessment must be undertaken to identify privacy risk and the mitigations to avoid such risk.

---

[3] https://ico.org.uk/media/action-weve-taken/mpns/2014217/gloucester-city-council-mpn-20170525.pdf

22. We are also aware of the growing number of health professionals who access the GP patient record such as health visitors and other specialist health professionals. However, we are also aware of some areas where access by non-health professionals, such as counsellors or third sector service providers as part of the Health and Social Care Partnership and we would caution against any wholesale access by such.

23. In terms of accessibility for the patient, the GDPR encourages data controllers, where possible, to provide remote access to a secure system which would provide individuals with direct access to their personal data. Until that is possible, any new systems and processes, including any data sharing, must be able to deal with patients' requests for access to their own data.

24. Where data sharing is taking place, all such activity must be controlled via a formal data sharing agreement that conforms to the ICO's Data Sharing Code of Practice[4].

We trust the Committee finds this response helpful. We would be happy to discuss any aspect of it further at the Committee's convenience if required.

[4] Data sharing code of practice, Information Commissioner's Office, May 2011 https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf