Witness Name: Emily Keaney
Statement No.: WITN7631001
Exhibits: 0
Dated: 22/12/2022

INFECTED BLOOD INQUIRY

WRITTEN STATEMENT OF EMILY KEANEY ON BEHALF OF THE INFORMATION COMMISSIONER'S OFFICE

I provide this statement in response to a request under Rule 9 of the Inquiry Rules 2006 dated 16 April 2021.

I, Emily Keaney, will say as follows:

Section 1: Introduction

1. I am the Deputy Commissioner, Regulatory Policy, in the Information Commissioner's Office (ICO). I am responsible[1] for overseeing the ICO's policy work programme, both domestically and internationally. I also oversee our work in responding to and preparing for major legislative change. I am not a member of any committees, associations, parties, societies or groups relevant to the Inquiry's Terms of Reference. This information is also available in my register of interest (RLIT0001945) published on the ICO's website.

[1] https://ico.org.uk/about-the-ico/who-we-are/management-board/

2. I have not provided evidence to, or have been involved in, any other inquiries, investigations or criminal or civil litigation in relation to human immunodeficiency virus ("HIV") and/or hepatitis B virus ("HBV") and/or hepatitis C virus ("HCV") infections and/or variant Creutzfeldt-Jakob disease ("vCJD") in blood and/or blood products.

3. The Information Commissioner's Office welcomes the opportunity to provide a statement to the Infected Blood Inquiry in response to questions regarding data protection and information governance. We wholeheartedly support the Inquiry's objectives to understand what happened and what processes could have led to men, women and children in the UK receiving infected blood which had far-reaching, and in many cases tragic, impact on them and their families. We would be interested in engaging with you on the outcomes of the Inquiry, especially the lessons that can be learned for the future, in connection with the use of information and people's personal data.

4. This aligns closely with the Information Commissioner's new strategy, ICO25 (RLIT0001946), which sets out our ambition to be a regulator which empowers people. In this respect, we want to empower people to be informed and have more control over their information and how it is used – to facilitate fairness, transparency, and accuracy of their records.

5. The ICO will be continuing to engage with and support stakeholders within the health and care landscape. This will include working with the NHS' Health and Care Information Governance panel and working group.

6. We have considered the questions you have sent us and below we provide our comments to those that relate to the legislation the Information Commissioner is responsible for.

7. The Information Commissioner has responsibility in the UK for promoting and enforcing the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018), the Freedom of Information Act 2000

(FOIA), the Re-Use of Public Sector Information Regulations 2015 (RPSI), the Environmental Information Regulations 2004 (EIR) and the Privacy and Electronic Communications Regulations 2003 (PECR), amongst others. We have set these out to help inform the Inquiry why we have not answered all your questions. This is because they fall outside of the Information Commissioner's responsibilities, for example those in relation to the Caldicott Guardians' principles.

8. The Commissioner is independent from 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 advice and guidance to individuals and organisations in complying with the law, particularly in their role as data controllers. The Commissioner also takes appropriate action where the law is broken.

Section 2

Evolution of the legislative framework

9. Whilst your questions to the ICO relate to the current framework, it is worth acknowledging the development of data protection legislation that has occurred since the period to which the Infected Blood Inquiry relates. It should be noted that the law has been different across the various periods the Inquiry is covering and that the current data protection legislation is not retrospective.

10. The first Data Protection Act introduced in 1983 included a range of data protection principles and rights for individuals in the UK. This legislation was updated in 1998 and most recently in 2018. It is important to note that data protection legislation has only ever applied to people who are living. The General Data Protection Regulation (now UK GDPR) also took effect in 2018 and introduced additional accountability principles and measures, including the requirement for public bodies to appoint a specialist data protection resource (Data Protection Officers).

11. Under the current UK GDPR and DPA 2018, a strong set of principles and requirements have now been established. Improvements in information rights are combined with enhanced regulatory powers, which allow the ICO to issue significant fines, reprimands, and corrective measures. Whilst the ICO signalled in June 2022 that we will only be issuing monetary fines to public sector organisations in the most serious cases, we still expect the high standards of data protection required by the legislation and will be increasing the use of the ICO's wider powers, including warnings, reprimands and enforcement notices.

12. We have history of taking robust action against healthcare organisations that have failed to meet the standards demanded of them when looking after their patients' data. For example, we issued a reprimand in 2022 to NHS Blood and Transplant Service (RLIT0001947) for a coding error that could have caused potential harm to people on the non-urgent transplant list.

13. Part of any strong framework must include support in the form of advice and guidance to controllers of personal data. The ICO has produced detailed guidance (RLIT0001948) to help organisations meet their obligations, providing details of what measures they should consider in order to comply with the law. This includes detailed guidance on issues experienced by the Inquiry such as securing data (RLIT0001949), and complying with the right of access (RLIT0001950).

14. Additionally, the ICO works with stakeholders from across the health and social care sector to improve the information governance and data protection guidance available to the system. As members of the Health and Social Care Information Governance Panel[2] we work alongside health sector stakeholders to streamline the healthcare specific guidance available via NHS England's Information Governance Portal[3].

[2] https://transform.england.nhs.uk/information-governance/health-and-care-information-governance-panel/
[3] https://transform.england.nhs.uk/information-governance/

Problems encountered by members of the public highlighted by the Inquiry

15. Thank you for providing details of the issues experienced by those involved in the Infected Blood Inquiry. We recognise the variety of data protection issues included within your presentation, however these have been broadly summarised as follows:
    i. Their records had been destroyed pursuant to destruction policies then in place.
    ii. Their records had been destroyed for other reasons (such as floods, fire or sewage spills).
    iii. Their records had been lost.
    iv. The request for disclosure of their medical records were ignored, or their access to their medical records was delayed.

16. For each of these circumstances there are corresponding principles and information rights set out in data protection legislation. In the law there is a duty on controllers to take responsibility for implementing processes in order to comply with these requirements and to adopt measures to mitigate data protection risks.

17. The ICO expects organisations to take steps to resolve these issues when they are identified, to restore the person's information rights, and to implement measures to reduce the risk of such incidents happening again.

Retention of information (Point i)

18. Many of the cases highlighted in the presentation (Inquiry Presentation Note on the Destruction and Retention of Medical Records INQY0000378) relate to investigations and requests for data after the standard retention periods had elapsed. We understand that GP records may contain a complete longitudinal record or a summary of an individual's healthcare. But certain hospital records for individual treatments are only required to be kept for eight years,

as set out in the current NHS Records Management Code of Practice (RLIT0001284).

19. Data protection legislation does not specify an exact period data must be held for, stating only that data should be held for no longer than is necessary for the purposes for which the personal data are processed. This is the principle of Storage Limitation (RLIT0001951)

20. The ICO encourages the development of guidance or codes of practice (such as the NHS Records Management Code of Practice) which standardises retention periods, based on the type of data and the purpose for which it is being retained. Clear retention policies reduce the burden on controllers, as they simplify processes when determining when data should be deleted or retained. It also improves the handling of subject access requests, as it should be clear to controllers what information they hold about people.

21. When developing a retention schedule, there should be an assessment of the level of risk of retaining personal data, balancing the requirement to store information for future use against the principles of storage limitation and data minimisation. Data should not be held 'just in case' as this could increase the likelihood of other data protection risks, such as the loss of unnecessarily held data causing inadvertent harms elsewhere.

22. Retention periods should also be reviewed regularly. If new risks are identified or if there are new requirements to store information, it is appropriate to amend retention schedules. We note the current NHS Records Management Code of Practice already instructs organisations to retain information that is still held that may be within scope of the Infected Blood Inquiry.

23. It is our view that the existing data protection framework provides sufficient flexibility for healthcare organisations or sector guidelines to define appropriate retention periods which strike the balance between record keeping and the principle of storage limitation.

Security of information in storage (integrity) (Point ii and iii)

24. There are many practical measures that healthcare organisations can take to improve the systems that hold their patient records and keep them safe (such as the digitisation of paper-based records). Drivers behind these measures include the cost of storing historic paper-based records remotely and the time it may take to process subject access requests (SARs) for this remotely held information. Current data protection legislation also places a demand on healthcare organisations to continually identify and manage the risks associated with storing and securing special category personal data.

25. The 6th principle of UK GDPR states that data should be processed (*which includes storage*) in a manner that ensures appropriate security of the personal data. This includes security issues identified in the presentation, such as protection against unauthorised alteration, accidental loss, destruction or damage.

26. The legislation does not define the level of security that should be in place for the storage of patient records. However, it requires controllers to have a level of security that is 'appropriate' to the risks presented by the processing.

27. Incidents where data is lost, destroyed or altered are considered a data protection breach in the legislation. The UK GDPR places a duty on all organisations to report certain personal data breaches to the ICO within 72 hours of becoming aware of the breach.

28. The ICO expects that any breach report should include a description of any steps taken to deal with the personal data breach and a description of the measures taken to mitigate any possible adverse effects. Organisations that experience a data breach should review their processes and take appropriate action to minimise the risk of such incidents happening again.

29. Failure to notify the ICO within 72 hours of a breach, or otherwise respond to a data protection breach, could result in regulatory action from the ICO.

Subject Access Rights

30. Individuals have the right to access and receive a copy of their personal data. This is referred to as a subject access request or 'SAR (Subject Access Request)'. Access rights have been enhanced from 2018 under UK GDPR, which states that organisations must provide this information free of charge with 30 days of receiving the request.

31. Healthcare organisations within scope of the Inquiry should be familiar with SARs and have established processes to ensure that they are dealt with in a timely manner. Our guidance (RLIT0001952) highlights ways in which this can be achieved, which includes training staff on how to recognise and handle a request.

32. We routinely deal with SAR issues though the ICO's complaints procedure. Although we are unable to advise if any of the complaints we have received relate directly to the Infected Blood Inquiry, we do provide advice and guidance to healthcare organisations on resolving SAR complaints and improving handling processes. In appropriate cases, the ICO may also exercise its enforcement powers against a controller or processor if they fail to respond to requests for information via this access route.

ICO complaints procedure

33. Anyone affected by the issues highlighted in the presentation has the right to lodge a complaint with the ICO. The ICO has a duty to investigate these complaints and can demand that organisations take steps to resolve them. Under the current legislation we may make recommendations to the organisation about how they can improve their information rights practices. In serious cases we may also use our regulatory powers, depending on the scale and nature of the infringement.

Summary

34. I hope this response provides the Inquiry with assurance that the current framework for data protection provides opportunities to resolve issues relating to the storage, access, and accuracy of medical records.

35. The ICO would also welcome clarity on whether there is a further requirement to work together here. In any case, we would be particularly interested in understanding any fundamental problems uncovered by this Inquiry, for example, concerning access requests to records. If there are, we would like to work with the Inquiry to understand the issues in greater depth and see where further guidance or other action may be required, which could have benefits for people facing similar barriers in the future.

Statement of Truth

I believe that the facts stated in this witness statement are true.

Signed _Emily Keaney_____

Dated _22/12/2022_____

Table of exhibits:

Date	Notes/ Description	Exhibit number
06/07/2022	ICO Register of Interests	RLIT0001945
07/11/2022	ICO25 Commissioners foreword	RLIT0001946
30/06/2022	Article titled 'ICO sets out revised approach to public sector	RLIT0001947

	enforcement’	
14/10/2022	ICO guide to GDPR	RLIT0001948
14/10/2022	ICO security guide	RLIT0001949
03/01/2022 (web access date)	ICO Right of Access	RLIT0001950
	Inquiry Presentation Note on the Destruction and Retention of Medical Records	INQY0000378
	NHS Records Management Code of Practice	RLIT0001284
14/10/2022	ICO storage limitation	RLIT0001951
03/01/2022 (web access date)	ICO Right of Access - ‘how should be prepare?’	RLIT0001952