Information Commissioner's Office

Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524 510 www.ico.org.uk

[redacted]
Information Governance Delivery Manager
Information Governance Directorate
Royal Free London NHS Foundation Trust
Anne Bryans House
77 Fleet Road
London
NW3 2QH

By email only to: [redacted]

10 November 2022

Dear [redacted]

Case reference: INV/0136/2022
Your reference: IGAR338

I write to inform you that the ICO has now completed its investigation into the loss of access to hysteroscopy scans held on USB sticks by Royal Free London NHS Foundation Trust ("the Trust").

In summary, it is my understanding that scans were saved on to a series of three USB sticks over a period of nine years from May 2013 until the remaining two encrypted USB sticks became inaccessible on 5 April 2018. It is unknown whether this inaccessibility was as a result of a technical failure of the USBs or human error from inputting the wrong password.

This case has been considered under the United Kingdom General Data Protection Regulation (the UK GDPR) due to the nature of the processing involved.

Our consideration of this case

I have investigated whether the Trust has complied with the requirements of the data protection legislation.

In the course of my investigation I have noted that there appears to be no actual harm caused by the failure and there was an element of human error and/or technological failure which contributed to this incident.

We have also considered and welcome the remedial steps taken by the Trust in light of this incident. In particular that the Trust has begun an overhaul of policies and procedures and investment in the Information Governance Team along with a Trust wide information asset mapping, USB stick review and the

identification and training of information asset owners. It is also noted that the Trust has ceased storing images on a USB and is reviewing the need to capture images going forward.

However, after careful consideration and based on the information provided, we have decided to issue the Trust with a reprimand in accordance with Article 58 of the UK GDPR.

Details of reprimand

The reprimand has been issued to the Trust in respect of the following infringements of the UK GDPR:

- Article 5(1)(f) which states that "Personal data shall be: (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

- Article 24(1) which states that "Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary."

In particular, the Trust has failed to ensure an appropriate level of security of personal data, resulting in the inaccessibility of personal data relating to between 4,000 to 10,000 data subjects. It is also noted that the Trust did not initially recognise this inaccessibility as a data protection breach resulting in a delay in reporting this to the ICO.

It has been noted that over the course of the use of the USBs the data held on this was not backed up on to Trust servers which was in breach of Trust policy. However whilst a breach of policy, there was a failure on the part of the Trust to raise awareness of the correct handling procedures for such devices as per policy, and a lack of oversight to ensure the policies in place were being correctly adhered to.

The Trust has been unable to evidence any risk assessments being completed over a nine year period, beyond a very basic set of considerations when the USBs were first commissioned and there was a Trust wide misconception of what constitutes a data breach. Furthermore, there was a lack of training in place, which resulted in a significant delay in both Information Governance and the ICO being informed of the breach. Finally there was a failure to adequately manage the use of the USBs sticks by appointing Information Asset Owners and System managers. Had such measures been in place, the Trust may have been able to prevent such an incident from occurring.

In conclusion, a reprimand is being issued due to infringements noted in respect of Article 5(1)(f) Article 24(1) of the UK GDPR.

Further Action Recommended

The Commissioner recommends that the Trust could take certain steps to improve its compliance with Article 5 (1)(f) and Article 24 (1) of the UK GDPR. In particular:

1. Review data protection training to ensure that employees are clear on what constitutes a data breach and when it needs to be reported.

2. Consider incorporating anonymised examples of incidents into data protection training to raise awareness of the potential for breaches to occur, with particular attention being given to their inclusion in departments or hospitals where such incidents have occurred.

3. Ensure that the collective learnings from data breaches are shared across the whole Trust, particularly if the type of processing is common across areas.

4. Ensure that any data processing activities are regularly and adequately risk assessed.

5. Ensure that Information Asset Owners are named and recorded for all Information Assets

6. Ensure that all Information Asset Owners confirm they have read and understood any relevant policies on a regular basis.

7. The trust could also ensure ongoing compliance with Article 33 by reviewing the data breach reporting procedure to ensure that the content is adequate and relevant to all departments within the Trust. Consider routinely recirculating the procedure with a requirement for all members of staff to confirm that they have read and understood the content.

In order to ensure that the above measures have been carried out, please provide an update with regards to your progress against the measures by 10 February 2023.

Whilst the above measures are suggestions, I would like to point out that if further information relating to this subject comes to light, or if any further incidents or complaints are reported to us, we will revisit this matter and further formal regulatory action may be considered as a result.

Further information about compliance with the data protection legislation which is relevant to this case can be found at the following link:

https://ico.org.uk/for-organisations/guide-to-data-protection/

We actively publicise our regulatory activity and outcomes, as this helps us to achieve our strategic aims in upholding information rights in the public interest. We may publish information about cases reported to us, for example where we think there is an opportunity for other organisations to learn or where the case highlights a risk or novel issue.

Therefore, we may publish the outcome of this investigation to publicise our regulatory authority and new powers under the UK GDPR. We will publish information in accordance with our Communicating Regulatory and Enforcement Activity Policy, which is available online at the following link:

https://ico.org.uk/media/about-the-ico/policiesandprocedures/1890/ico_enforcement_communications_policy.pdf

Please let us know if you have any concerns about this.

Thank you for your co-operation and assistance during the course of our investigation.

We now consider the matter closed.

Yours sincerely

[redacted]
Investigation Officer - Civil Investigations
Regulatory Supervision Service
The Information Commissioner's Office
[redacted]

Please note that we are often asked for copies of the correspondence we exchange with third parties. We are subject to all of the laws we deal with, including the United Kingdom General Data Protection Regulation, the Data Protection Act 2018 and the Freedom of Information Act 2000. You can read about these on our website (www.ico.org.uk).

The ICO publishes basic details about the complaints, investigations and self-reported data breaches it handles. These details include the name of the organisation concerned, the dates that we opened and closed the case, and the outcome. Examples of published data sets can be found at this link (https://ico.org.uk/about-the-ico/our-information/complaints-and-concerns-data-sets/).

We do not include personal data in the published datasets and will anonymise the names of sole traders etc prior to publication. We also do not publish cases concerning domestic CCTV complaints and may not publish certain other cases if we feel it is not appropriate to do so in the circumstances.

If you wish to raise an objection to us publishing a case in the datasets, whether or not we have published it yet, please contact us explaining your reasons for this at icoaccessinformation@ico.org.uk .

Please say whether you consider any of the information you send us is confidential. You should also say why so that we can take that into consideration. However, please note that we will only withhold information where there is good reason to do so.

For information about what we do with personal data see our privacy notice at www.ico.org.uk/privacy-notice