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 Manager
University Hospitals Bristol and Weston NHS Foundation Trust
Trust Headquarters
Marlborough Street
Bristol
BN1 3NU

By email only to: [redacted]

7 March 2023

Dear [redacted]

Case Reference Number: INV/0609/2021

Previous Case Reference Number: IC-96299-J8N9

I write to inform you that the ICO has now completed its investigation into the loss of access to patient records held on an Electronic Document Viewing System by University Hospital Bristol and Weston NHS Foundation Trust ("the Trust").

In summary, it is my understanding that patient records were saved on to an Electronic Document Viewing System. The Trust decided to terminate the use of this system and the records on it were downloaded prior to allowing the system licence to expire. However this download was not fully successful but this was not investigated prior to the licence expiry and therefore a number of records became inaccessible and some permanently lost.

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 the planning of care of one patient was impacted due to the inaccessibility of patient records although there was no actual harm to the patient care. 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 drafted an Information Asset Management policy to include sections on decommissioning information assets. It is also noted that the Trust has developed a new decommissioning process which will include investigations into anomalies in downloads prior to allowing licenses to expire.

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."

- Article 24(2) which states that "Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller."

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 1159 data subjects. 1155 data subjects records were inaccessible from 19 January 2020 until 12 October 2021, whilst partial records of 4 patients amounting to 115

pages were permanently deleted. It is also noted that the Trust did not have an appropriate decommissioning policy in place at the time of the breach.

It has been noted that there was a lack of policy or procedure in place to ensure the appropriate oversight was in place for the personal data concerned. The failure to do so has meant that the licence expired and rendered personal data either inaccessible or permanently deleted.

Furthermore, the inaccessibility of the personal data has meant a detrimental effect on one patient's care, and there is the potential that there could be further impacts in the future.

In conclusion, a reprimand is being issued due to infringements noted in respect of Article 5(1)(f), Article 24(1) and Article 24(2) 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), Article 24(1) and Article 24(2) of the UK GDPR. In particular:

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

2. Ensure that a decommissioning policy is drafted, implemented and circulated to all relevant staff.

3. Ensure that the decommissioning policy includes a requirement to complete an adequate risk assessment prior to decommissioning a system or allowing a licence to expire.

4. Ensure that the decommissioning policy includes a requirement to review any extract of data to ensure that it is complete and accurate before any system is decommissioned or a licence is allowed to expire.

5. Ensure that the decommissioning policy allows for any discrepancies that are found instigating an immediate risk assessment and investigation.

6. Ensure that the decommissioning policy allows for any discrepancies that are found to be resolved before any system is decommissioned or a licence is allowed to expire.

7. Ensure that any new or updated policies or procedures are regularly circulated to staff.

8. Ensure that all case management systems are regularly risk assessed.

We understand that measures 7 and 8 have already been carried out. In order to ensure that the remaining measures have been carried out, please provide an update with regards to your progress against the measures by 14 April 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