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]

By email only to: [redacted]

29 June 2022

Dear [redacted]

Case Reference Number INV/0963/2021.

I write to inform you that the ICO has now completed its investigation into the incident regarding Allied Health Professionals (AHP) accidentally making data accessible to health care providers when data subjects had not given consent for this data to be shared.

In summary, it is my understanding that the incident occurred when the IT provider, Infotex, made unexpected changes to AHP's systems. As the changes were not agreed and were unknown by AHP, they were not identified as part of AHP's routine testing. As a result this meant that the data of 2573 of AHPs' patients were made accessible to health care providers which was against the consent of the patients.

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 AHP has complied with the requirements of data protection legislation.

In the course of the investigation, I have noted that there was a lack of sufficient change management process documents in place at the time of the incident. It has also been established that there wasn't a sufficient contract in place with AHP's data processor, Infotex, outlining the necessary data protection clauses and requirements. However, it has been noted that this matter has been fully

investigated and all data subjects have been informed of the incident following audits that highlighted the extent of the issue.

We have also considered and welcome the remedial steps taken by AHP in light of this incident. In particular, the introduction of a processing contract with Infotex, which will allow AHP to comply with their UK GDPR article 28 obligations. Further to this the review of the Infotex contracts will ensure that chances of this incident occurring again in the future are diminished.

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

Details of reprimand

The reprimand has been issued in respect of the following processing operations that have infringed the UK GDPR:

- Article 6, (1)(a) UK GDPR states – "Processing shall be lawful only if and to the extent that at least one of the following applies:
  (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes.

In particular, AHP did not have a suitable policy or contracts in place to ensure that the consent could be given or not given by patients. The contracts and change management process that AHP had in place with Infotex were not suitable for the changes being made to the system and this led to the error in question not being noticed through testing before the changes were placed onto the system. If the contract and change management process had been sufficient then the likelihood of this incident occurring would have been diminished as the Infotex employee would have been clearer of what was expected of them and the mistake would have likely have been noticed in the testing phase. The result of these failings by AHP is that patient data has been accessible contrary to patient wishes and in contravention of Article 6 (1)(a).

Further Action Recommended

The Commissioner recommends that AHP could take certain steps to improve compliance with UK GDPR. In particular:

1. Continue to check all contracts with data processors to ensure that they are legally compliant.

2. Ensure that all future change management documents are clear and specific on the changes that are to be made.

3. Ensure that all staff are aware of this incident and that remedial measures taken as a result of this incident continue to be implemented.

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]

[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 accessicoinformation@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