Upholding information rights

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

[redacted]
Warrington and Halton Teaching Hospitals NHS Foundation Trust

By email only to: [redacted]

27 May 2022

Dear [redacted]

Case Reference Number: INV/0055/2022
Data Security Incident: 26882

I write to inform you that the ICO has now completed its investigation into the incident when a copy of a data subject's form had been uploaded to another individual's records and was subsequently released to that patient's family.

In summary, it is my understanding that an appointments administrator uploaded a patient's urgent referral form to the wrong patient's notes. A response to a subject access request contained these notes so special category personal data of another individual was revealed to the recipient. The affected data subject contacted Warrington and Halton Hospitals NHS Foundation Trust's (WHH) complaints team after the individual that made the subject access request contacted the affected data subject and informed them of the disclosure. The form was seven pages long and contained full personal demographic details of the patient, full details of the reason for referral, details of family medical history, patient medication and clinical history.

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

We have investigated whether WHH has complied with the requirements of data protection legislation.

In the course of my investigation we have noted that:

- At the time of the incident, the [redacted] team didn't check any subject access request responses taken from the main patient administration system. WHH confirmed that these are computer generated PDFs and can

contain between 1-6000 pages and WHH's [redacted] Department did not have the capacity to check these.

- WHH confirmed that there were no policies, written procedures or guidance which set out how documents such as referral forms should be uploaded onto records or any specific mention to double check the correct record was being updated.
- WHH confirmed that there was an Access to Health Records policy but that that this policy did not include a process for checking subject access request responses for either paper or electronic notes.
- This incident did not therefore breach any policy or procedure. There may have been an element of human error due to the similarities to the patients' names but having a process in place would have reduced the chance of this happening.
- WHH confirmed that a Data Protection Impact Assessment (DPIA) had not been conducted into the subject access request process as it is not regarded as high-risk processing. The ICO considers that responding to subject access requests in a healthcare environment should usually be considered high-risk and therefore warrants serious consideration of a DPIA.
- WHH confirmed that there was no impact or delay on clinical treatment or appointments and the referral was managed in the correct way.

We have also considered and welcome the remedial steps taken by WHH in light of this incident. In particular:

- The records were corrected at the time the incident was reported.
- An action plan for this incident was produced.
- The standard operating procedure for requests for records has been updated to include a two-tier process of checking medical records.
- A monthly audit has been implemented to assess the robustness of the new process.
- The Access to Health Records policy is being reviewed and updated as a whole to ensure the processes around how records are requested and shared are more robust.
- [redacted] staff attended a briefing session to understand the updated process.
- Since the incident WHH has added a process whereby an incident report is created for all mis-files detected in records.

However, after careful consideration and based on the information provided, we have decided to issue WHH 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/DPA 2018:

- **Article 5(1)(f) – Security**
  The UK GDPR requires data controllers to process personal data securely by means of appropriate technical and organisational measures. There was no checking process in place in relation to subject access request responses within the [redacted] department either for paper or electronic notes or any process to identify misfiled records. WHH has stated that "this means that although the staff members in the [redacted]Team were following the process in place, this process was not robust." The lack of checking processes in place was a failing and an infringement of Article 5(1)(f).

- **Article 5(1)(d) – Accuracy**
  The UK GDPR requires data controllers to ensure that the personal data it processes remains accurate and up to date in line with the purposes for which it is being processed. In this case one patient had the incorrect letter on their electronic record and the other was missing the letter from their record resulting in both records being inaccurate or incomplete. The issue that caused the inaccuracies was the uploading of the letter onto the incorrect record. WHH has confirmed that there was no policy, written procedure or guidance which set out how documents such as referral forms should be uploaded onto records or any expectation to double check the correct record was being updated. The lack of measures to prevent inaccurate records for both individuals were infringements of Article 5(1)(d).

The ICO has noted that WHH mentioned that some of the computer generated PDFs can contain between 1-6000 pages and initially suggested that WHH's [redacted] Department does not have the capacity to check these. I would like to refer you to the ICO's guidance in relation to whether a subject access request is "manifestly excessive" in case you consider an exemption may apply. However,

please note that a request is not necessarily excessive just because the individual requests a large amount of information.

When can we refuse to comply with a request? | ICO

Further Action Recommended

The Commissioner recommends that WHH considers taking certain steps to improve compliance with UK GDPR/DPA2018. In particular:

1. Satisfy yourselves that sufficient checks are built into your procedures to make sure the correct case has been selected when uploading documents. This should help to ensure records remain accurate and complete.

2. Ensure relevant staff are aware of the updated standard operating procedure in relation to subject access request responses and the requirement for a two-tier process of checking medical records.

3. Complete a DPIA in relation to subject access request processes and responses, assess the level of risk in such processing and implement measures that can be put in place to mitigate any such risks.

4. Review the content and frequency of your data protection training to ensure that sufficient practical guidance is given to staff in how to comply with data protection legislation so that awareness is embedded within WHH. Consider your methods of monitoring and ensuring staff who deal with personal data complete this and refresh their training regularly.

Please provide an update with regards to your progress on the above steps within the next six months and no later than 27 November 2022.

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 may 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 case closed.

Yours sincerely

[redacted]
Information Commissioner's Office
[redacted]

For information about what we do with personal data see our privacy notice

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