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 and DPO
Epsom & St Helier University Hospitals NHS Trust
St Helier Hospital
Wrythe Lane
Carshalton
Surrey SM5 1AA
By email only to: [redacted]

7 April 2022

Dear [redacted]

Our Current Case Reference Number INV/1627/2020
Our Previous Case Reference Number IC-74546-Y3G1
Your NHS Data Security Incident 22290

I write to inform you that the ICO has now completed its investigation into the personal data breach you notified us of on 2 December 2020.

In summary, it is my understanding that incorrect test result data was passed by Epsom & St Helier University Hospitals NHS Trust (the Trust) to Public Health England (PHE) resulting in individuals erroneously being contacted via the NHS Test and Trace (NHS T&T) system and advised to isolate.

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

For more information about our powers under the current data protection legislation please see the attached leaflet.

- ICO Enforcement leaflet – UK GDPR and DPA 2018

Our consideration of this case

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

The incident was caused by action taken by an individual member of Trust staff in an attempt to resolve an identified anomaly by means other than reinstating the coding that had earlier been removed from a report by a colleague. The change made to that coding within the report was following a consultant's request to remove what was considered to be a duplicate comment entry. The

change implemented caused test results to be falsely reported as positive. In turn, this resulted in individuals who had been in contact with the affected data subjects also being advised via the NHS T&T system to isolate. The required isolation of all affected individuals resulted in the one-day closure of three local schools (including one special needs school) and one special needs nursery.

In the course of my investigation I have noted the following mitigating factors:

- It is acknowledged that there was no error in the Trust's COVID testing process; their internal recording of test results; or the test results given directly to Trust staff. The error was introduced when the test results were incorporated into the reports used to transmit the data to SGSS.

- The pandemic response to COVID introduced a new requirement for the reporting of negative test results. [redacted]

- The member of Trust staff was aware of the purpose of the code and was uncertain that the action he was taking would be successful. It is noted that he requested checks be undertaken by PHE and their response was considered to be affirmative.

- The Trust attempted to correspond with PHE in relation to the incident [redacted]

- The Trust stated that the SGSS reporting mechanism did not allow their staff to see the results that would be automatically produced which meant they could not check it themselves.

We have also considered and welcome the remedial steps taken by the Trust in light of this incident. In particular it is noted that

- The Trust acted swiftly and appropriately in managing the incident to limit, as far as they were able, the impact which had resulted;

- The Microbiology Computing Policy and Protocol has been updated;

- No formal complaints were received in relation to the incident, other than the calls made to the Trust relating to the erroneous positive COVID test results which have not been recorded by the Trust as complaints.

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 GDPR.

Details of reprimand

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

- Article 5(1)(f) which states that personal data shall be "*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 32(1)(b) and (d) which state "*Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:*

  (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

  (d) a process for regular testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing."

In particular, the Trust did not have adequate policies and procedures in place as summarised below:

- The Trust stated that an individual member of staff was the single point of contact within the Microbiology department who was aware, prior to the incident occurring, that there was an alternative purpose for the duplication of the negative comment code, being one of two recipients of email guidance from PHE.

- The Trust stated there was no formal policy or procedure to explain to staff how the receipt of this type of information should be recorded or made available to relevant employees. The information contained within the email is considered significant and the failure of the Trust to have a policy or procedure in place for adequate receipt recording and communication cascade is considered to be an aggravating factor in the incident occurring. Had the information within the email, or the email itself, been shared with colleagues it is considered likely that the incident would have been avoided.

- From the information provided it is considered that the Trust made a change to a live environment without any prior or adequate testing in a safe space or without adequate and appropriate consultation with PHE. A failure to adequately test both the initial, and subsequent coding changes, meant that an opportunity to address the anomalies prior to the changes being implemented was missed.

- Notwithstanding the unique circumstances of the pandemic reporting requirement, and PHE's utilisation of an existing report for a new purpose, the evidence indicates that at least one member of Trust staff was aware that there was the potential for the automatically transmitted results to be misinterpreted by the SGSS. Given the potential consequences of incorrect data being provided to PHE, and against the backdrop of the pandemic, the investigation has determined that the Trust had insufficient controls and documented procedures in place to address such a risk.

- [redacted], the investigation into this incident has highlighted opportunities where tighter enforcement of coding amendments and enhanced colleague communication could have prevented the incident from occurring.

- As a result of the incident occurring there was significant impact upon a number of Trust patients and staff: staff were detrimentally affected as the actual negative results had to be re-confirmed before they could remain at/arrive for work; surgical procedures were postponed and delayed; as a result of contract tracing several schools and nurseries had to close (two of which were special needs facilities) with the associated wider ranging impact this will have had on parents. The Trust could be considered fortunate that no clinical harm came to any of the affected patients as a result of the incident and that the school and nursery closures were for a limited time. However it is noted that the potential for significant detriment was substantial.

It has also been noted through the course of the investigation that that although the SGSS was set up on-site by PHE's Field Service Team in replacement of a

previous system, there is no formal contract or data sharing agreement in place between the Trust and PHE in respect of use of SGSS. Furthermore, a Data Protection Impact Assessment (DPIA) had not been completed. This is considered to represent a weakness and to be a concern in respect of data protection compliance.

When considering the Articles cited above, and in particular Article 32, as a data controller responsible for the medical wellbeing of patients and staff, appropriate consideration should have been given by the Trust to the potential risks associated with their failure to ensure the ongoing integrity and resilience of their data processing systems when implementing coding amendments in a live environment. While it is considered that the Trust has demonstrated an ability to take remedial action to rectify the coding processing deficiencies, it did not have effective measures in place to ensure the ongoing integrity and resilience of processing systems in compliance with Article 5(1)(f) and 32(1)(b).

Further Action Recommended

The Commissioner recommends that the Trust could take certain steps to improve compliance with current data protection legislation ie UK GDPR. In particular:

1. The Trust should implement a procedure for the recording and cascading of information received externally in order to reduce the reliance on the knowledge held by one operational member of staff. Information in relation to the impact of coding changes should be shared with consultants and clinicians for consideration when requests for amendments are received.

2. Risk analysis should be built into change management procedures for coding changes in order to adequately safeguard personal information.

3. The Trust should undertake a Data Protection Impact Assessment (DPIA) to ensure that the process involved in this incident is properly documented and compliant with current data protection legislation.

4. The Trust should consider implementing a test environment in which all coding amendments are robustly checked prior to implementation. For situations where reports are required to be sent externally, all reasonable attempts should be made to identify areas of risk and adequate steps taken to mitigate those risks prior to live implementation.

5. The ICO's audit report published in September 2021 identified that the Trust had a lack of controls in place to ensure that all staff had read and

understood key data protection and security related policies. The Trust should ensure that appropriate action is taken to address this.

6. The ICO's audit also identified a lack of information sharing agreements in place for data sharing arrangements. In light of this incident, the Trust should consider contacting PHE to discuss the implementation of a formal arrangement for SGSS processing.

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]
Lead Case Officer – Civil Investigations

Regulatory Supervision Service
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 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