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

NHS Blood and Transplant (NHSBT)
500 North Bristol Park
Northway
Filton
Bristol
BS34 7QH

By email only to: [redacted]
cc: [redacted]

Date: 9 May 2022

Dear [redacted]

Case Reference Number: INV/0501/2020

Thank you for your latest correspondence to the ICO of 26 January 2022. In this, you provided a response to the ICO's further enquiries in respect of NHSBT's representations of 7 December 2021.

I write to inform you that the ICO has now reached a final decision in respect of its investigation into INV/0501/2020.

The incident at the centre of this investigation concerns the inadvertent integration of untested development code for a future liver scheme into NHSBT's live environment. This integration error led to a number of prospective transplant patients being excluded from NHSBT's Liver Matching Run (LMR) between 11 and 18 September 2019.

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

Our consideration of this case

Key compliance issues

As you are aware, the ICO previously submitted a Notice of Intent (NOI) to NHSBT on 9 November 2021. This outlined the Commissioner's intention to issue NHSBT with an administrative fine of £749,856 for infringements of Article 32 of the GDPR. It has been determined that it is not necessary to issue an administrative fine to NHSBT. Rather, it has

been decided that a reprimand would be appropriate. This letter sets out the reason for that decision.

You will be aware that the Commissioner found that NHSBT had failed to implement sufficient technical and organisational measures to ensure a level of security appropriate to the risk to the integrity, availability and resilience of its transplant matching systems.

Significant contributing factors to the above infringements include:

a. a lack of appropriate branch or version control to ensure that developers could not unknowingly introduce untested code into NHSBT's live environment;

b. a lack appropriate peer reviewing of developers' work to reduce the likelihood of inadvertent coding errors being introduced;

c. inadequate knowledge and understanding by all relevant staff members as to the scope of regression testing required prior to the launch of new organ matching schemes into NHSBT's live environment; and

d. a lack of appropriate training for staff in respect of code testing, branch control and the use of peer review.

It is considered that taking such steps would have reduced the likelihood of the incident occurring.

The contraventions in this case involved data belonging to vulnerable individuals; namely those awaiting an organ transplant. NHSBT's failure to properly process such data could result in data subjects not being offered lifesaving treatment.

In this case, a total of five data subjects are identified as having been directly affected by the incident - ie they were not offered potential liver transplants during the relevant breach period as intended. Three of these patients experienced delays in receiving a liver transplant. The remaining two patients were in fact not well enough to receive a liver transplant had it been offered in the relevant period.

As per the ICO's NOI, it is considered that the gravity of the incident extends beyond those directly affected, as the risk of detriment to other patients on the LMR was equally high. This is because there was the

potential for further individuals to have received liver matches during the time of the coding defect.

Further, the coding merge caused a total of four unforeseen, yet 'critical', defects within NHSBT's live environment which could have affected an even greater number of individuals.

The ICO also notes that the LMR omissions error only appears to have come to light following an external transplant centre query. It therefore cannot be discounted that a higher number of patients could have missed liver transplant offers over a longer period of time had this communication not occurred.

Mitigating factors and remedial action

As referenced within its NOI, the ICO has considered and welcomes the measures taken by NHSBT to mitigate the risk of further damage being caused to affected data subjects. These measures include:

a. Halting further code releases into NHSBT's live environment until an assurance review of its testing procedures on each of the 27 systems directly impacting patient safety had been undertaken.

b. Contracting a specialist consultancy to independently verify the framework NHSBT uses to simulate the full test lifecycle and process for code releases.

c. Making an immediate policy change to regression test all organ allocation schemes for every release, even where no changes are due to be made for any organ type. These tests were to be conducted by NHSBT's highly specialised Statistics Team.

d. Informing affected data subjects and/or their family members of the incident via Duty of Candour letters, alongside offers by NHSBT's clinical team to meet with data subjects and/or their family members to discuss the incident in more detail and address any outstanding concerns.

e. Prioritising patients who had missed liver transplant offers in the relevant breach period where it was deemed appropriate for them to undertake a procedure.

Investigation outcome

After careful consideration and based on the information provided to date, the Commissioner hereby confirms that he will not be proceeding with formal enforcement action against NHSBT in relation to the alleged contraventions of the of the GDPR as detailed within the NOI dated 9 November 2021. As explained in the opening paragraph of this letter, that means that an administrative fine will not be issued to NHSBT in connection with this matter.

However, the Commissioner has decided to issue NHSBT with a reprimand in accordance with Article 58 of the GDPR. To confirm, this reprimand has been issued in respect of the following processing operations that have infringed the GDPR:

- **Article 32 (1)(b) – Security of processing**

  This states:

  '1. 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 and the processor 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'.

The basis of this reprimand is as outlined earlier in this letter under the sub-heading 'key compliance issues'.

Further action recommended

Alongside the ICO's decision to issue NHSBT with a reprimand in this case, the Commissioner also recommends that NHSBT takes certain steps to improve its compliance with the (UK) GDPR and implement sufficient technical and organisational measures to ensure a level of security appropriate to the risk to the integrity, availability and resilience of its transplant matching systems.

Information Commissioner's Office

In particular:

1. Ensure that all remedial measures set out in NHSBT's Root Cause Analysis (RCA) action plan are completed.

   In particular, it is noted that Action 13 - to review MPD1226 to ensure this is fit for purpose and amended accordingly - remains outstanding.

   Note: A copy of the latest RCA action plan provided to the ICO has been attached to this letter for your viewing.

2. Ensure that appropriate training is provided to internal staff (and external contractors as necessary) in respect of NHSBT's established branch control and testing procedures for code development and release at appropriate intervals.

3. Ensure that mandatory data protection training is undertaken by supplier provided contractors where such roles require access to/have the potential to impact NHSBT data.

For completeness, we ask that NHSBT provides a progress update to the ICO on the above recommendations in six months' time, or by no later than **9 November 2022**. Unless otherwise instructed, please provide this update to [redacted]

It must be emphasised that the ICO's decision to issue a reprimand in this case does not detract from the seriousness of this incident, and has been reached on the balance of all information available to our office prior to and following NHSBT's legal representations.

Therefore, whilst the above measures are suggestions, I would like to point out that if further information relating to this incident comes to light, or if any further incidents or complaints of a similar nature are reported to us, we will revisit this matter and 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%20ico/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]
Lead Case Officer
Civil Investigations
Regulatory Supervision Service
The Information Commissioner's Office

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.