Royal Devon University Healthcare NHS Foundation Trust

Trust Personal Data Breaches

Reference Number: RDF2367-24
Date of Response: 28/03/24

Further to your Freedom of Information Act (FOIA) request, please find the Trust's response(s):

Please provide the following details for the time period 1st January 2022- 1st January 2024

1. *How many personal data breaches occurred within your organisation?*

   Please see response after Question 4.

2. *How many personal data beaches were reported to the ICO?*

   Section 22 – Future Publication
   Trust can confirm that it holds information that you have requested. This information is exempt under Section 22 of the Freedom of Information Act because the information is intended to be published in the near future.

   Section 21
   This information is also exempt under Section 21 of the Freedom of Information Act because it is reasonably accessible to you. The information you requested can be accessed via the following link:

   The Trust published this information for each financial year in our Annual Report and Accounts document (please search for 'Information Commissioner'), available at the link below:

   https://www.royaldevon.nhs.uk/about-us/publications/reports-and-trust-documents/

3. *Of those reported to the ICO, how many were reported within 72 hours of the organisation being aware of the breach?*

   Please see response after Question 4.

4. *What is the main cause of personal data breaches within your organisation? i.e. Unauthorised access to information systems, unauthorised access/ permissions, unauthorised or accidental access to data, unauthorised or accidental alteration of data, unauthorised or accidental disclosure of data, unauthorised or accidental loss of data.*

   The Trust exempts disclosure of the requested information under Section 31(1) & (3) of the FOIA.

   Section 31(1) of the Freedom of Information Act allows a public authority to exempt information if its disclosure would or would be likely to prejudice the prevention or detection of crime and the exercise of its functions, including securing the health, safety and welfare of persons. Section 31(3) of the Freedom of Information Act allows a public authority to neither confirm nor deny whether it holds information where such confirmation would be likely to prejudice any of the matters outlined in

section 31(1). This includes information the disclosure of which would, or would be likely to, prejudice the prevention or detection of crime.

Section 31 is subject to a public interest test for determining whether the public interest lies in withholding the information or not.

Public interest test

When balancing the public interest, RDUH must consider whether the information should be released into the public domain. Arguments need to be weighed against each other.

The most persuasive reason for disclosing the information would be openness and transparency; the Trust rightly should be accountable for how it manages personal data and have appropriate processes in place for managing when a data incident or breach occurs.

This must be weighed against the strongest reason for non-disclosure which is the fact that the Trust's IT infrastructure and information security would likely be placed at risk if information in respect of personal data breaches was to be placed into the public domain, endangering individuals, and their healthcare information we are entrusted with. The Trust considers that to release this information could highlight potential vulnerabilities, increasing the risk of cyber-attacks and/or other forms of criminal activity. This information can also be used to compare to other organisations which in turn can aid criminals in identifying more vulnerable targets.

Cyber-attacks which may amount to criminal offences under the Computer Misuse Act 1990 or the Data Protection Act 2018, are rated as a Tier 1 threat by the UK Government. Our Trust, like any organisation may be subject to cyber-attacks and since it holds large amounts of sensitive, personal, and confidential information, maintaining the security of this information is extremely important.

In this context, the Trust considers that providing the requested information would also provide information about the Trust's information systems and its resilience to cyber-attacks. There is a very strong public interest in preventing the Trust's information systems from being subject to cyber-attacks. Releasing the information requested would be likely to prejudice the prevention of cybercrime and this is not in the public interest.

As an Operator of Essential Services:
(https://www.legislation.gov.uk/uksi/2018/506/schedule/2/paragraph/8),
the Trust must comply with The Network and Information Systems Regulations 2018. By releasing information that could increase the likelihood or severity of a cyber-attack, the Trust would fail to meet its security duties as stated in section 10 (https://www.legislation.gov.uk/uksi/2018/506/regulation/10) of the Network and Information Systems Regulations 2018.

The prejudice in complying with Section 31(3) of FOIA is real and significant and would allow valuable insight into the perceived strengths and weaknesses of the Trust's information security, IT infrastructure and information systems.

In respect of our transparency obligations, we can confirm that the Trust does have robust measures in place for reporting, handling, identifying and responding to personal data incidents and breaches. The Trust is accountable to the ICO and NHS England and completes the DSP Toolkit: https://www.dsptoolkit.nhs.uk/OrganisationSearch/RH8.

On balance, we have concluded that the public interest in disclosing the information is outweighed by that of withholding the information.