Our Ref: 688

October 2024

Doncaster and Bassetlaw Teaching Hospitals NHS Foundation Trust

Freedom of Information Act Request

Dear Doncaster and Bassetlaw Teaching Hospitals NHS Foundation Trust,

Data breach incidents

- How many data breaches has your organisation experienced in the past 36 months from today's date?
- What types of data (e.g., personal, financial, health records) were compromised in these breaches, if any occurred?
- Did any of these breaches include ransomware attacks?

Data protection and backup strategies

- How frequently does your organisation back up critical data and systems?
- Are backups stored in an immutable format to prevent tampering or encryption by malicious actors?
- Do you plan to apply Zero Trust best practices to your backup storage strategy?
- Which backup management software and backup storage solutions do you use?

Response and recovery

- Do you have an incident response plan, and do you regularly use it?
- How long did it take you to recover following a breach or ransomware attack?
- What percentage of data was recovered?

Please note that all information related to the security processes involved in protecting the Trust's data systems is considered exempt from disclosure under section 24(1) (Safeguarding National Security) of the Freedom of Information Act. If disclosed, such information could be used to identify ways in which our computer systems could be breached. Patient data as well as other confidential information could therefore be accessed or compromised. The Trust has a duty to protect such information under the Data Protection Act.

As part of the Critical National Infrastructure for the NHS, the Trust has a duty to protect the integrity of our systems. The disclosure of the information requested could expose weaknesses in our systems and lead to breaches, making the UK or its citizens, in this case our patients, more vulnerable to security threat. The release of such information is therefore exempt under s. 24 (1) (Safeguarding National Security) of the Freedom of Information Act.

Section 24 is a qualified exemption, therefore the public interest in withholding the information should outweigh the public interest in its disclosure. The Trust has applied the public interest test and believes that disclosure of this information could lead to breaches in Trust security and is therefore a reasonable threat to the confidential patient data held on our systems. There is a strong public interest in protecting the confidentiality of patient data and of ensuring that healthcare services can be provided to the public without increasing the possibility of attack by hackers or malware, or of putting personal or other information held on these systems at risk of corruption or subject to illegal access. For these reasons, the Trust has decided that it is in the public interest to withhold this information at this time.

Additionally, the information is also being withheld by the Trust for organisational security reasons; and we consider that the information which has been withheld is also exempt from disclosure under section 31(1)(a) of the Freedom of Information Act.

The relevant parts of the ICO guidance on the subject (https://ico.org.uk/media/for-organisations/documents/1207/law-enforcement-foi-section-31.pdf) are described as follows:

31.—(1) Information is exempt if its disclosure under this Act would, or would be likely to, prejudice - (a) the prevention or detection of crime.

As Section 31 is subject to the prejudice test the Trust reasoning for its use is to withhold information that would make anyone, including the public authority itself, more vulnerable to crime for example, by disclosing its own security procedures.

It is the view of our Information Security function together with the Department for Information Governance, Caldicott & SIRO Support that the disclosure of the information requested would prejudice our ability to resist any future cyber and related attacks, etc. on our systems.

In view of the above, the Trust exempts the supply of the information requested.

If you are not satisfied with the handling of your request, you have the right to request an internal review. Requests for an internal review should be submitted within 40 working days from the date of this response, and should

be addressed to: [Internal review contact details].

If you remain dissatisfied after the internal review, you have the right to appeal to the Information Commissioner's Office (ICO). The ICO can be contacted at:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Tel: 0303 123 1113
Website: https://ico.org.uk/make-a-complaint/

Our Ref: 688

October 2024

Doncaster and Bassetlaw Teaching Hospitals
NHS Foundation Trust

Our Ref: 688

October 2024

Doncaster and Bassetlaw Teaching Hospitals
NHS Foundation Trust