Our Ref: 482
July 2024

Doncaster and Bassetlaw Teaching Hospitals
NHS Foundation Trust

Freedom of Information Act Request

1. How many cyber incidents (threat and breach) occurred in the last two years (1st of July 2022-1st of July 2024)? None

2. For each of the following cyber incident types, please indicate if your organisation experienced them in any month from the 1st of July 2022- 1st of July 2024. If yes, specify the month(s) in which they occurred:

Phishing attacks: Yes/No. If yes, which month(s)?
Ransomware attacks: Yes/No. If yes, which month(s)?
Distributed Denial of Service (DDoS) attacks: Yes/No. If yes, which month(s)?
Data breaches: Yes/No. If yes, which month(s)?
Malware attacks: Yes/No. If yes, which month(s)?
Insider attacks: Yes/No. If yes, which month(s)?
Cloud security incidents: Yes/No. If yes, which month(s)?
Social engineering attacks (excluding phishing): Yes/No. If yes, which month(s)?
Zero-day exploits: Yes/No. If yes, which month(s)

We are applying Section 31 subsection 1 (a), which is allowed under the Freedom of Information Act 2000. This exempts disclosure of information which is prejudicial to law enforcement and the prevention or detection of crime. If disclosed into the public domain, this information would constitute a risk to security.

It is important to appreciate that a disclosure to a request from a single applicant is not viewed in law as a disclosure to just that person, but a release of information into the public domain which when released cannot be reclaimed or rolled back. Hence we feel that the risk is significant that release of such information would be likely to prejudice law enforcement.

This exemption does require a test of whether the public interest lies in disclosing or withholding the information in question. The test did not find any factors which significantly aided the public's understanding of current issues or decisions taken, or which would demonstrate competence, transparency and accountability for public expenditure. In contrast, releasing information on security systems and processes would pose a significant risk to security and integrity from unauthorised access as well as security of individuals. This would seriously compromise the ability of this Trust to function and undermine public confidence in the Trust. This is therefore considered sensitive information which falls within the Freedom of information Act 2000 exemption at section 31:

- disclosure of details of successful attacks would increase any potential vulnerability to cyber-attack and increase the risk of future successful

attacks;

- disclosure would provide a malicious third party with information which may assist them in carrying out a criminal act against a public body

(including the institution concerned);

- hackers or other malicious parties may draw upon information gathered from a wide range of sources to derive information about an organisation's

cyber security arrangements;

Details of successful attacks would provide useful confirmation to malicious third parties about which of their methods of attack have been successful.

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 d.wraith@nhs.net.

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/

3. For each of the following supplier types, please indicate if any cyber incidents related to them occurred between the 1st of July 2022-1st of July 2024. If yes, specify the volume of cyber incidents that occurred:

IT service providers: Yes/No
Medical equipment suppliers: Yes/No
Software vendors: Yes/No
Cloud service providers: Yes/No
Data storage/management companies: Yes/No
Telecommunications providers: Yes/No
Security service providers: Yes/No
Managed service providers (MSPs): Yes/No
Third-party payment processors: Yes/No

We are applying Section 31 subsection 1 (a), which is allowed under the Freedom of Information Act 2000. This exempts disclosure of information which is prejudicial to law enforcement and the prevention or detection of crime. If disclosed into the public domain, this information would

constitute a risk to security.

It is important to appreciate that a disclosure to a request from a single applicant is not viewed in law as a disclosure to just that person, but a release of information into the public domain which when released cannot be reclaimed or rolled back. Hence we feel that the risk is significant that release of such information would be likely to prejudice law enforcement.

This exemption does require a test of whether the public interest lies in disclosing or withholding the information in question. The test did not find any factors which significantly aided the public's understanding of current issues or decisions taken, or which would demonstrate competence, transparency and accountability for public expenditure. In contrast, releasing information on security systems and processes would pose a significant risk to security and integrity from unauthorised access as well as security of individuals. This would seriously compromise the ability of this Trust to function and undermine public confidence in the Trust. This is therefore considered sensitive information which falls within the Freedom of information Act 2000 exemption at section 31:

- disclosure of details of successful attacks would increase any potential vulnerability to cyber-attack and increase the risk of future successful

attacks;

- disclosure would provide a malicious third party with information which may assist them in carrying out a criminal act against a public body

(including the institution concerned);

- hackers or other malicious parties may draw upon information gathered from a wide range of sources to derive information about an organisation's

cyber security arrangements;

Details of successful attacks would provide useful confirmation to malicious third parties about which of their methods of attack have been successful.

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 d.wraith@nhs.net.

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

Our Ref: 482
July 2024

Doncaster and Bassetlaw Teaching Hospitals
NHS Foundation Trust

SK9 5AF
Tel: 0303 123 1113
Website: https://ico.org.uk/make-a-complaint/

4. During the period from 1st of July 2022 -1st of July 2024, did your organisation experience any of the following impacts due to cyber incidents?

Were any appointments rescheduled due to cyber incidents? Yes/No No

Was there any system downtime lasting more than 1 hour? Yes/No No
Did any data breaches occur? Yes/No No
Were any patients affected by data breaches? Yes/No No