The Clatterbridge Cancer Centre
NHS Foundation Trust

Clatterbridge Road
Bebington
Wirral
CH63 4JY

Tel: 0151 556 5000
Web: www.clatterbridgecc.nhs.uk

Date: 23 September 2021

Re: Freedom of Information Request
Ref: 262-2021

Thank you for your email dated the 31st August 2021, requesting information in relation to ransomware incidents.

The information that you require is as follows:

1. **In the past three years has your organisation:**
    a. **Had any ransomware incidents? (An incident where an attacker attempted to, or successfully, encrypted a computing device within your organisation with the aim of extorting a payment or action in order to decrypt the device?)**
        i. **If yes, how many?**
    b. **Had any data rendered permanently inaccessible by a ransomware incident (i.e. some data was not able to be restored from back up.)**
    c. **Had any data rendered permanently inaccessible by a systems or equipment failure (i.e. some data was not able to be restored from back up.)**
    d. **Paid a ransom due to a ransomware incident / to obtain a decryption key or tool?**
        i. **If yes was the decryption successful, with all files recovered?**
    e. **Used a free decryption key or tool (e.g. from https://www.nomoreransom.org/)?**

i. **If yes was the decryption successful, with all files recovered?**

f. **Had a formal policy on ransomware payment?**
   i. **If yes please provide, or link, to all versions relevant to the 3 year period.**

g. **Held meetings where policy on paying ransomware was discussed?**

h. **Paid consultancy fees for malware, ransomware, or system intrusion investigation**
   i. **If yes at what cost in each year?**

i. **Used existing support contracts for malware, ransomware, or system intrusion investigation?**

j. **Requested central government support for malware, ransomware, or system intrusion investigation?**

k. **Paid for data recovery services?**
   i. **If yes at what cost in each year?**

l. **Used existing contracts for data recovery services?**

m. **Replaced IT infrastructure such as servers that have been compromised by malware?**
   i. **If yes at what cost in each year?**

n. **Replaced IT endpoints such as PCs, Laptops, Mobile devices that have been compromised by malware?**
   i. **If yes at what cost in each year?**

o. **Lost data due to portable electronic devices being mislaid, lost or destroyed?**
   i. **If yes how many incidents in each year?**

Exempt under Section 31(1a) - The prevention or detection of crime

We have carefully considered your request and although we hold the information we have concluded that we will not be able to provide you with the information you have requested and we will rely on the exemption under Section 31(1a) - The prevention or detection of crime of the Freedom of Information Act 2000 ("the Act").

Section 31(1a) the Act provides that information is exempt from disclosure if the information would or would be likely to prejudice law enforcement

and the prevention or detection of crime by making the Trust vulnerable to criminal activity through cyber security attacks.

The Trust, as a public body is mindful that in order to engage this exemption, we must demonstrate that disclosure of the information would, or would be likely to, prejudice the prevention of crime.

The term "would …prejudice" has been defined as it is more likely than not to occur whereas "would likely….prejudice" is a lower threshold. The Trust has applied the prejudice test under Section 31, and we are content that the requirements of the test have been met.

Having reached the conclusion that the prejudice test has been met, we have also considered whether the public interest in maintaining the exemption outweighs the public interest in disclosure.

<u>Public Interest Test</u>
Factors favouring disclosure

- **The Trust recognises that answering the request would promote openness and transparency with regards to the Trust's IT security**

Factors in favour of non-disclosure

- **Increased risk of Cyber-attacks, which may amount to criminal offences under the Computer Misuse Act 1990 or the Data Protection Act 2018. Cyber-attacks are rated as a Tier 1 threat by the UK Government. Cyber-attacks could result in:**
    - **Breaches in Trust security and is therefore a reasonable threat to the confidential patient data held on our systems**
    - **Temporary or long term lack of availability of IT systems**
    - **Corruption/loss of patient data which would prevent or interrupt provision of patient care**
- **Disclosure of the information would assist a hacker in gaining valuable information as to the nature of the Trust's systems, defences and possible vulnerabilities**

Having carefully considered the public interest test we have concluded that 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

Taking the above into consideration, having applied the necessary, relevant tests and taking all the current circumstances into consideration we are content that the requirements of all necessary and relevant tests have been met and the application of the exemption under Section 31(1a) is appropriate on this occasion.

2. **Does your organisation use a cloud based office suite system such as Google Workspace (Formerly G Suite) or Microsoft's Office 365?**
   Our Trust uses the NHS Mail Hybrid Office 365 Solution.
   a. **If yes is this system's data independently backed up, separately from that platform's own tools?**
      Yes, this system's data is independently backed up.

3. **Is an offsite data back-up a system in place for the following? (Offsite backup is the replication of the data to a server which is separated geographically from the system's normal operating location site.)**
   An offsite data back-up a system in place for the highlighted:
   a) **Mobile devices such as phones and tablet computers**
   b. **Desktop and laptop computers**
   c. **Virtual desktops**
   d. **Servers on premise**
   e. **Co-located or hosted servers**
   f. **Cloud hosted servers**
   g. **Virtual machines**
   h. **Data in SaaS applications**
   i. **ERP / finance system**
   j. **We do not use any offsite back-up systems**

4. **Are the services in question 3 backed up by a single system or are multiple systems used?**
   Single System

5. **Do you have a cloud migration strategy? - No**
   a) **If so is there specific budget allocated to this? N/A**

6. **How many Software as a Services (SaaS) applications are in place within your organisation?**
   5
   a) **How many have been adopted since January 2020?**
      2

Should you require any further information please do not hesitate to contact me on the email address provided below.

Please remember to quote the reference number above in any future communications.

If you are dissatisfied with the handling of your request, you have the right to ask for this to be investigated internally.

If you are dissatisfied with the information you have received, you have the right to ask for an internal review.

Both processes will be handled in accordance with our Trust's Freedom of Information Policy and the Freedom of Information Act 2000.

Internal investigation and internal review requests should be submitted within two months of the date of receipt of the response to your original letter and should be addressed to: Freedom of Information Review, The Clatterbridge Cancer Centre NHS Foundation Trust, Clatterbridge Road, Bebington, Wirral, CH63 4JY

If you are not satisfied with the outcome of the internal investigation/review, you have the right to apply directly to the Information Commissioner for a decision. The Information Commissioner can be contacted at: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

In order for us to ensure customer satisfaction and to monitor compliance with the Freedom of Information Act 2000, we would be grateful if you could take a couple of minutes to complete a short feedback form via the link below:

https://www.surveymonkey.co.uk/r/H39RFMM