The Clatterbridge Cancer Centre
NHS Foundation Trust

Clatterbridge Road
Bebington
Wirral
CH63 4JY

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

Date: 10 December 2020

Re: Freedom of Information Request
Ref: 266-2020

Thank you for your email dated the 12th November 2020, requesting information in relation to cyber attacks since 2015.

The information that you require is as follows:

Under the FOI Act 2000, I would like to request the following:

A list of all cyber-attacks (both failed and successful) on NHS hospitals falling under your remit, in each year since 2015 (including broader cyber-attacks which include these hospitals). Where possible, please could you split the data as follows:

- **Ideally, I am requesting only those cyber-attacks identified as or suspected of a) coming from a source within Russia or China; or b) emanating from any individual(s) or group(s) known to have, or suspected of having, links to the Russian or Chinese state. In each instance, please could you make clear which country the attack relates to.**
- **If this is not possible, please could you make clear whether an attack is thought to have come from inside/outside the UK.**

In each instance, I am also requesting the following information:

- **The severity of the attack, where it has been noted (e.g. low, medium, high).**
- **The outcome of successful attacks. For example: were documents stolen (and how many)? Was confidential data stolen (and how much)? Were any operations or other NHS processes cancelled or delayed as a result (and how many)?**
- **The cost to the NHS, where that cost is easily deductible/accessible. This could include but is not limited to a) delayed or cancelled operations, lost data, etc.; b) the security/staffing cost of defending against an attack; c) any consequent legal costs e.g. lawsuits filed successfully against the NHS as a result of personal data theft. If this part of the request is unduly onerous, please disregard.**

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.

Public Interest Test

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.

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.