Our Ref: 297/2020
November 2020

NHS
Doncaster and Bassetlaw Teaching Hospitals
NHS Foundation Trust

Re: Your request made under the Freedom of Information Act 2000

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.

Under section 31(3) of the FOIA (http://www.legislation.gov.uk/ukpga/2000/36/section/31), we can neither confirm nor deny whether information is held.

S31(3) of the FOIA 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.

As section 31(3) is a qualified exemption, it is subject to a public interest test for determining whether the public interest lies in confirming whether the information is held or not.

Factors in favour of confirming or denying the information is held:

We consider that to confirm or deny whether the requested information is held would indicate the prevalence of cyber-attacks against our IT infrastructure, and would reveal details about our information security systems.

We recognise that answering the request would promote openness and transparency with regards to our IT security.

Factors in favour of neither confirming nor denying the information is held:

Cyber-attacks, which may amount to criminal offences for example under the Computer Misuse Act 1990 or the Data Protection Act 1998, are rated as a Tier 1 threat by the UK Government.

Like any organisation, the Trust may be subject to cyber-attacks; and because we hold large amounts of sensitive, personal and confidential information, maintaining the security of this information is extremely important.

In this context, we consider that confirming or denying whether the requested information is held would provide information about the Trust's information security systems and its resilience to cyber-attacks.

There is a very strong public interest in preventing our information systems from being subject to cyber-attacks. Confirming or denying the type of information requested would be likely to prejudice the prevention of cybercrime, and this is not in the public interest.

We consider that if we were to confirm or deny whether we hold the requested information, it would enable potential cyber attackers to ascertain how and to what extend the Trust is able to detect and deal with ICT security attacks. Our position is that complying with the duty to confirm or deny whether the information is held would be likely to prejudice the prevention or detection of crime, as the information would assist those who want to attack the Trust's IT systems.

Disclosure of the information would assist a hacker in gaining valuable information as to the nature of our IT systems, defences and possible vulnerabilities. This information would enter the public domain and set a precedent for other similar requests which would, in principle, result in the Trust being a position where it would be more difficult to refuse information in similar requests. To confirm or deny whether the information is held is likely to enable hackers to obtain information in mosaic form combined with other information to enable hackers to gain greater insight than they would ordinarily have, which would facilitate the commissioning of crime, such as hacking itself and also fraud. This would impact on our operations including front line services. The prejudice in complying with section 1(1)(a) FOIA is real and significant as to confirm or deny would allow valuable insight into the perceived strengths and weaknesses of our IT systems.