Nottingham and Nottinghamshire Integrated Care Board

08/11/2023

NN-ICB/23/477

Dear Requestor

RE: Freedom of Information Request

With reference to your request for information I can confirm in accordance with Section 1 (1) of the Freedom of Information Act 2000 that we partially hold the information that you have requested. A response to each part of your request is below and attached.

In the request you asked:

1. Can you please list the number of devices deployed by your organisation for the following?

   Device Type

   - Desktop PCs
   - Laptops
   - Mobile Phones
   - Printers
   - Multi Functional Devices (MFDs)
   - Tablets
   - Physical Servers
   - Storage Devices (for example: NAS, SAN)
   - Networking Infrastructure (for example: Switches, Routers, Interfaces, Wireless Access Points)
   - Security Infrastructure (for example: Firewalls, Intrusion Detection Systems (IDS), Virus Monitoring Tools)

2. Does your organisation have any plans to procure below software applications, if yes then please provide required information in the below format?

   Application Name

   - Digital Electronic Discharge Systems
   - Maternity Information Systems
   - Laboratory Information Management System

3. Can your organisation provide Clinical ICT Strategy key decisions and priorities or ICT strategy documents for present and future years?
4. Does your organisation use Artificial Intelligence and Robotics, if yes then please list the services and their estimated cost for 23/24 and 24/25?
5. Can your organisation provide planned ICT procurement plans across software, hardware or services for current and future years? (Software Applications/Hardware Devices/IT Managed Services)

As requested, please see attached completed Excel spreadsheet in response to the above request.

In response to one part of Question 1.

1. Can you please list the number of devices deployed by your organisation for the following?
    - Security Infrastructure (for example: Firewalls, Intrusion Detection Systems (IDS), Virus Monitoring Tools)

Section 31(1)(a)

Exempt information under Section 31(1)(a) of the Freedom of Information Act 2000 for the following reasons:

Our organisation may be subject to cyber-attacks and, since it holds sensitive, personal and confidential information, maintaining the security of this information is extremely important. 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.

Section 31(1)(a) says that a public authority does not have to disclose information under section 1 Freedom of Information Act 2000 where doing so would or would be likely to prejudice the functions of law enforcement, in this case, the prevention or detection of crime.

In this context, providing the requested information would provide information about 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. Providing the type of information requested would be likely to provide attackers with information relating to the state of our cyber security defences, and this is not in the public interest.

Prejudice Test

In engaging this exemption, it is necessary to consider the prejudice test as followed by the Information Commissioner's Office.

Applicable interests

In this case the request relates to details about the ICB's Security Infrastructure (for example: Firewalls, Intrusion Detection Systems (IDS), Virus Monitoring Tools).

The ICB considers that the release of this information would or would be likely to put the ICB at risk of being targeted by cyber criminals as it would reveal information about the specific IT systems/software used and would or would be likely to allow cyber criminals to target the specific system vulnerabilities to gain unlawful access to information. This could compromise sensitive information held by the ICB and make it more vulnerable to crime.

Any disclosure made under the Freedom of Information Act, is deemed to be made to the public at large. There is a risk that this information could be used for criminal activity either on its own or together with other information in a mosaic effect which increases the risk of prejudice to the prevention of crime.

The nature of the prejudice

The prejudice that may result must be "real, actual or of substance" and there must be a causal link between the disclosure and the potential prejudice. The prejudice in this case is the ICB's ability to prevent unlawful access, theft, vandalism to its systems and safeguard the data held in those systems.

As a public authority the ICB is a potential target for cyber criminals. Disclosing information about the specific systems, software or hardware used would or would be likely to provide cyber criminals with information needed to gain unlawful access to information held by the ICB, such as personal data held about patients as well as employees. Furthermore, the ICB also holds commercially sensitive information

that, on balance, would or would be likely to cause prejudice to the ICB financially, contractually and reputationally if unlawfully accessed. The real and actual prejudice described would or would be likely to cause a detrimental effect to patients as well as to the business interests and reputation of the ICB.

The causal link between the disclosure under the Freedom of Information request to the prejudice that would or would likely be caused has been demonstrated above. To confirm, placing such information into the public domain weakens the security of the ICB's systems and, therefore, its ability to sufficiently protect the data it holds.

The likelihood of prejudice

The ICB has demonstrated that there is a real and significant risk that the prejudice in relation to the unlawful access to systems would or would be likely to occur.

In undertaking the prejudice test, the ICB considers that the above prejudice and subsequent harm/damage would or would be likely to occur if the information were disclosed.

The Information Commissioners Office Prejudice Test guidance - https://ico.org.uk/media/for-organisations/documents/1214/the_prejudice_test.pdf states the following.

- *'Would' therefore means 'more probable than not'; in other words, there is a more than 50% chance of the disclosure causing the prejudice, even though it is not absolutely certain that it would do so.*
- *'would be likely' means that there must be more than a hypothetical or remote possibility of prejudice occurring; there must be a real and significant risk of prejudice, even though the probability of prejudice occurring is less than 50%.*

In taking all of the above into account, the ICB concludes that the likelihood of prejudice would cause harm if the information was disclosed.

Public Interest Test

The Information Commissioners Office states:

- *Section 31 is a prejudice based exemption and is subject to the public interest test. This means that not only does the information have to prejudice one of the purposes listed, but, before the information can be withheld, the public interest in preventing that prejudice must outweigh the public interest in disclosure.*

A public interest test was undertaken on the 7 November in response to your request made under the Freedom of Information Act 2000.

Factors favouring disclosure

The ICB recognises that disclosure of the information sought in relation to the ICB's Security Infrastructure would promote accountability and transparency about how the organisation and the NHS in general perform our functions.

Factors favouring non-disclosure

Conversely to the factors demonstrated above in favour of disclosing the information sought in relation to the ICB's Security Infrastructure, there is an inherent public interest in protecting the ability of public authorities to enforce the law and therefore protect society from crime. There is public interest in complying with the ICB's legal obligations to keep personal data secure and to take appropriate measures which includes keeping areas confidential where necessary.

On balance of the factors considered above, along with relevant case law, we conclude that the ICB would be entitled to withhold information relating to the ICB's Security Infrastructure and that this would not be superseded by public interest considerations.

If you are unhappy with the way in which your request has been handled, NHS Nottingham and Nottinghamshire Integrated Care Board (ICB) have an internal review procedure through which you can raise any concerns you might have. Further details of this procedure can be obtained by contacting Lucy Branson, Associate Director of Governance via lucy.branson@nhs.net or by writing to FOI Team at NHS Nottingham and Nottinghamshire ICB, Sir John Robinson House, Sir John Robinson Way, Arnold, Daybrook, Nottingham, NG5 6DA.

If you remain dissatisfied with the outcome of the internal review, you can apply to the Information Commissioner's Office (ICO), who will consider whether the organisation has complied with its obligations under the Act and can require the organisation to remedy any problems. Generally, the ICO cannot make a decision unless you have exhausted the complaints procedure provided by NHS Nottingham and Nottinghamshire ICB. You can find out more about how to do this, and about the Act in general, on the Information Commissioner's Office website at: https://ico.org.uk/for-the-public/

Complaints to the Information Commissioner's Office should be sent to:

FOI/EIR Complaints Resolution, Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF. Telephone 0303 123 1113 or report a concern via https://ico.org.uk/concerns/

Yours sincerely

Freedom of Information (FOI) Officer on behalf of *NHS Nottingham and Nottinghamshire Integrated Care Board*

notts.foi@nhs.net