County Durham and Darlington NHS
NHS Foundation Trust

Executive Corridor
Darlington Memorial Hospital
Hollyhurst Road
Darlington
DL3 6HX
Switchboard Tel: 01325 38 0100
Foundation Trust Office: 01325 74 3625
Corporate Records Office: 01325 74 3700

Request for Information Reference: 11.21.49

FOI Direct line: 01325 743700
Email: cdda-tr.cddftfoi@nhs.net

Email only

21st December 2021

Freedom of Information Act 2000 – Request for Information

Thank you for submitting a request for information which we received on 24th November 2021 in relation to County Durham and Darlington NHS Foundation Trust (the Trust). Your request has been processed under the provisions of the Freedom of Information Act 2000 and I am now able to provide you with a response.

Your request was in relation to Information Technology and I am providing the following information in response to your specific questions:

1. **Do you have a formal IT security strategy? (Please provide a link to the strategy)**
   a) **Yes**
   b) **No** – No (The Trust has a Health Informatics Strategy)

2. **Does this strategy specifically address the monitoring of network attached device configurations to identify any malicious or non-malicious change to the device configuration?**
   a) **Yes**
   b) **No** – No
   c) **Don’t know**

3. **If yes to Question 2, how do you manage this identification process – is it:**
   a) **Totally automated – all configuration changes are identified and flagged without manual intervention.**
   b) **Semi-automated – it’s a mixture of manual processes and tools that help track and identify configuration changes.**
   c) **Mainly manual – most elements of the identification of configuration changes are manual.**

   Not Applicable

4. **Have you ever encountered a situation where user services have been disrupted due to an accidental/non malicious change that had been made to a device configuration?**
   a) **Yes** – Yes
   b) **No**
   c) **Don't know**

5. **If a piece of malware was maliciously uploaded to a device on your network, how quickly do you think it would be identified and isolated?**
   a) **Immediately** – Yes
   b) **Within days**
   c) **Within weeks**
   d) **Not sure**

6. **How many devices do you have attached to your network that require monitoring?**

   Approximately 11000

   a) **Physical Servers:** 47
   b) **PC's & Notebooks: record number:** 6500

7. **Have you ever discovered devices attached to the network that you weren't previously aware of?**
   a) **Yes** – Yes
   b) **No**
   If yes, how do you manage this identification process – is it:

   a) **Totally automated – all device configuration changes are identified and flagged without manual intervention.**
   b) **Semi-automated – it's a mixture of manual processes and tools that help track and identify unplanned device configuration changes.**
   c) **Mainly manual – most elements of the identification of unexpected device configuration changes are manual.**

   The Trust is unable to provide a response to your request due to its legal requirement under part 3 section 10, (1, 2) of The Network and Information Systems Regulations 2018 (NISR), to protect information about the security of our networks. This prevents the disclosure of the information you have requested as it would require us to breach the responsibility we have under the NISR.

   As a result the Trust is refusing your request under section 31(1) of the FOIA which states that information is exempt if, under this Act, it would, or would be likely to prejudice (a) the prevention or detection of crime. If the Trust were to confirm or deny its identification method as, it could enable the perpetrators to understand how they could or could not have been detected and as such it could enable further attacks and the Trust would have failed to protect the security of the Trust systems.

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.

8. **How many physical devices (IP's) do you have attached to your network that require monitoring for configuration vulnerabilities?**

   11000

9. **Have you suffered any external security attacks that have used malware on a network attached device to help breach your security measures?**
   a) Never
   b) Not in the last 1-12 months
   c) Not in the last 12-36 months

   The Trust is unable to provide a response to your request due to its legal requirement under part 3 section 10, (1, 2) of The Network and Information Systems Regulations 2018 (NISR), to protect information about the security of our networks. This prevents the disclosure of the information you have requested as it would require us to breach the responsibility we have under the NISR.

   As a result the Trust is refusing your request under section 31(1) of the FOIA which states that information is exempt if, under this Act, it would, or would be likely to prejudice (a) the prevention or detection of crime. If the Trust were to confirm or deny if it had experienced a cyber-attack or provide the specific details of any cyber-attacks in the last three years, it could enable the perpetrators to understand if they had or had not been detected and as such it could enable further attacks and the Trust would have failed to protect the security of the Trust systems.

   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.

10. **Have you ever experienced service disruption to users due to an accidental, non-malicious change being made to device configurations?**
   a) Never
   b) Not in the last 1-12 months – Not in the last 1-12 months
   c) Not in the last 12-36 months

11. **When a scheduled audit takes place for the likes of PSN or Cyber Essentials, how likely are you to get significant numbers of audit fails relating to the status of the IT infrastructure?**
    a) **Never**
    b) **Occasionally**
    c) **Frequently**
    d) **Always**

    The Trust does not define the outputs of our audits as ‘Fails’. Each audit will produce recommendations, informational, minor, major or critical.

In line with the Information Commissioner’s directive on the disclosure of information under the Freedom of Information Act 2000 your request will form part of our disclosure log on the Trust’s website. However please be assured that we anonymise all responses prior to adding them to the disclosure log.

I hope that this response has provided you with the information you had requested. If you have any queries or wish to discuss the information supplied, please do not hesitate to contact me by telephone or in writing. If however, you are dissatisfied with the way in which your request has been handled and would like an internal review, you will need to contact me in writing at the above address or via cdda-tr.cddftfoi@nhs.

If you remain dissatisfied with our response following an internal review you have the right to appeal to The Information Commissioner at Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF. More information is available on their website; www.ico.gov.uk.

Yours sincerely

Corporate Records and Freedom of Information Facilitator