Request for information under the Freedom of Information Act – 2021.860
Released – 24 June 2021

Thank you for your email dated 8 June 2021 requesting information regarding medical devices.

Please find detailed below a summary of your original request together with our response.

Original request:

1. Have all devices, including medical devices, on the Trust's network been identified?

Yes

2. Does the Trust have a real-time Risk Register of all assets connected to its network?

Yes

3. Does the Trust identify and monitor all medical devices being used for remote patient management?

Not applicable

4. Does the Trust comply with the following assessments or security standards:

- Data Security and Protection Toolkit (DSPT)
- Cyber Essentials
- Cyber Essentials Plus
- The EU Security of Network & Information Systems (NIS) Directive
- ISO27001

Yes

5. Have you had any data compromises due to previously unknown connected medical devices in the last 5 years? If so, how many?
6. What percentage of your medical device estate is currently running on unsupported/end-of-life software?

The Kent Community Health NHS Foundation Trust can neither confirm nor deny whether the information requested for questions 5 and 6 is held under section 31(3) – Law Enforcement, of the Freedom of Information Act (FOIA). The full wording of section 31 can be found here:

http://www.legislation.gov.uk/ukpga/2000/36/section/31

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
The Trust considers that to confirm or deny whether the requested information is held would indicate the prevalence of cyber-attacks against the Trust's ICT infrastructure and would reveal details about the Trust's information security systems.

The Trust recognises that answering the request would promote openness and transparency with regards to the Trust's ICT 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 2018, are rated as a Tier 1 threat by the UK Government.

The Trust, like any organisation, may be subject to cyber-attacks and, since it holds large amounts of sensitive, personal and confidential information, maintaining the security of this information is extremely important.

In this context, the Trust considers 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 the Trust's 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.

Balancing the public interest factors
The Trust has considered that if it were to confirm or deny whether it holds the requested information, it would likely enable potential cyber attackers to ascertain how and to what extent the Trust is able to detect and deal with ICT security attacks. The Trust's 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 likely assist those who want to attack the Trust's ICT systems. Disclosure of the information would likely assist a hacker in gaining valuable information as to the nature of the Trust's 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 the Trust's operations including its 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 the Trust's ICT systems.

7. Approximately what percentage of your medical device estate is segregated from the main network?

100%

8. Does the Trust Board recognise the importance of IT device asset management and cyber security and allocate sufficient budgetary support?

This question appears to be asking for comment which we are not obliged to provide under the Freedom of Information Act.