

Ref: FOI/GS/ID 9302

Please reply to:
FOI Administrator
Trust Management
Maidstone Hospital
Hermitage Lane
Maidstone, Kent
ME16 9QQ
Email: mtw-tr.foiadmin@nhs.net
www.mtw.nhs.uk

20 August 2024

Freedom of Information Act 2000

I am writing in response to your request for information made under the Freedom of Information Act 2000 in relation to Clinical software systems.

You asked: All questions are shown as received by the Trust.

Please provide information regarding the use of the following clinical software systems at Maidstone and Tunbridge Wells NHS Trust:

- *EPR (Electronic Patient Record): An Electronic Patient Record (EPR) is a digital version of a patient's paper chart. EPRs are real-time, patient-centered records that make information available instantly and securely to authorized users.*
- *Patient Engagement Portal: A Patient Engagement Portal is an online platform that enables patients to interact with their healthcare providers, access their medical records, schedule appointments, and receive educational materials and support.*
- *Patient Access System: A Patient Access System allows patients to manage their appointments, access personal health information, and communicate with healthcare providers, enhancing their overall experience and engagement.*
- *Virtual Ward Software: Virtual Ward Software is used to manage and monitor patients remotely, typically those with chronic conditions or those recovering from surgery, to provide continuous care and reduce hospital admissions.*
- *Population Health Management Software: Population Health Management Software helps healthcare providers manage and analyze health data for a specific population to improve health outcomes, reduce costs, and enhance the patient experience.*
- *Contact Centre: Contact Centre software facilitates communication between patients and healthcare providers, managing inbound and outbound calls, emails, and other forms of communication efficiently.*

- *Telecare Software: Telecare Software provides remote care services to patients, using technology to monitor health conditions and support independent living, often for elderly or disabled individuals.*

For each clinical system listed above, please provide the following details where possible:

- a) System type:*
- b) Supplier name:*
- c) System name:*
- d) Date installed:*
- e) Supplier contract expiration:*
- f) Is this contract annually renewed? - Yes/No*
- g) Do you currently have plans to replace this system? - Yes/No*
- h) Procurement framework:*
- i) Other systems it integrates with:*
- j) Total value of contract (£):*
- k) Notes - e.g. we are currently out to tender:*
- l) Framework used:*
- l) If no system exists, what alternative do you use?*

Trust response:

The Trust can neither confirm nor deny whether information is held under section 31(3) of the 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 NHS Trust considers that to confirm or deny whether the requested information is held would indicate the prevalence of cyber- attacks against the NHS Trust's infrastructure and the level of detail poses a number of risks in respect of security and information. The NHS Trust recognises that answering the request would promote openness and transparency with regards to the NHS Trust's software systems.

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. The NHS 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 NHS Trust considers that confirming or denying whether the requested information is held would provide information about the NHS Trust's systems and its resilience to cyber-attacks. There is a very strong public interest in preventing the NHS 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 NHS Trust has considered that if it were to confirm or deny whether it holds the requested information, it would enable potential cyber attackers to ascertain how and to what extent the NHS Trust is able to detect and deal with security attacks. The NHS 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 assist those who want to attack the NHS Trust's systems. Disclosure of the information would assist a hacker in gaining valuable information as to the nature of the NHS 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 NHS Trust being in 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 NHS 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 NHS Trust's systems.