Maidstone and
Tunbridge Wells
NHS Trust

Ref: FOI/GS/ID 9357

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

30 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 Access control maintenance contract.

You asked: All questions are shown as received by the Trust.
Access Control System Overview:
1. Current System(s):
** What electronic access control system(s) do you currently have in place? Please include manufacturer of control unit & model (e.g. SALTO, PAXTON, ASSA)*
2. Access-Controlled Doors:
** How many doors across all of your sites have access control systems installed? How many per each site?*
3. Access Control Types:
** Please provide a detailed breakdown of the different types of access control setups in place (e.g., magnetic lock doors, electric strike doors, battery-operated electronic handle sets, battery-operated electronic cylinders, etc.).*
4. System Age:
** When was your current access control system installed? Which company installed it?*
5. System Integration:
** Is your access control system integrated with your ID card production or other systems (e.g., time and attendance, building management/CCTV and/or fire/security alarm systems)? If so, which system(s) is it integrated with?*
6. Supplier Information:
** What are the names of the suppliers of your existing access control system?*

** Who is your current supplier for access cards and fobs, and do you purchase these directly or through your access control installers/maintenance contractors?*

7. Manufacturer and Models:

** What manufacturer and model of cards and fobs do you use for your access control system? Please provide specific details of each of the exact manufacturer/model of card(s)/fob(s) that you use at each site (e.g. Paxton 692-052 Net2 Proximity ISO Cards Pack of 500 SKU: AC-PAX-692-052) together with the cost (including VAT) each month/year.*

8. Management Software:

** What software is used to manage the door controllers and readers in your access control system? (e.g. Paxton Net2 Pro)*

Usage and Distribution Details:

9. Consumable Usage:

** Please provide data on the monthly and annual usage/purchases of access control cards and fobs. This should include how many are issued, lost/replaced, and returned faulty/damaged each month/annum.*

10. User Information:

** How many individual users require access control cards/fobs across all sites? If possible, please provide a breakdown by site or building.*

Maintenance and Support:

11. Management and Contact Information:

** Who manages your site’s access control system? Please provide a name, direct email address and direct telephone number / extension for this contact.*

12. Support/Maintenance Contracts:

** Do you have a current support/maintenance contract for your access control system? If so, when does this contract expire?*

Future Plans:

13. Planned Changes:

** What are the organisations plans related to the installation, upgrade, or support/maintenance of access control systems over the next three to five years?*

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 extend 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 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.