Maidstone and Tunbridge Wells NHS Trust

Ref: FOI/GS/ID 9180

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

24 October 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 Firewall, Anti-virus, and Enterprise Agreement.

You asked: All questions are shown as received by the Trust.
1. Standard Firewall (Network) - Firewall service protects your corporate Network from unauthorised access and other Internet security threats
2. Anti-virus Software Application - Anti-virus software is a program or set of programs that are designed to prevent, search for, detect, and remove software viruses, and other malicious software like worms, trojans, adware, and more.
3. Microsoft Enterprise Agreement - is a volume licensing package offered by Microsoft.
The information I require is around the procurement side and we do not require any specifics (serial numbers, models, location) that could bring threat/harm to the organisation.
For each of the different types of cyber security services can you please provide me with:
a. Who is the existing supplier for this contract?
b. What does the organisation annually spend for each of the contracts?
c. What is the description of the services provided for each contract?
d. Primary Brand (ONLY APPLIES TO CONTRACT 1&2)
e. What is the expiry date of each contract?
f. What is the start date of each contract?
g. What is the contract duration of the contract?
h. The responsible contract officer for each of the contracts above? Full name, job title, contact number and direct email address.
i. Number of Licenses (ONLY APPLIES TO CONTRACT 3)

Trust response:
Following the recent Synnovis cyber-attack the Trust has taken the decision to refuse to release information relating to our essential systems and software. 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.