NHS
South East Coast
Ambulance Service
NHS Foundation Trust

Trust Headquarters
Nexus House
Gatwick Road
Crawley
West Sussex
RH10 9BG

Tel: 0300 123 0999
www.secamb.nhs.uk

30th November 2020

Email:

Dear,

I am writing in response to your enquiry under the Freedom of Information Act 2000 (FOIA) reference FOI 20/10/18.

You requested the following information, please also see our response below:

Under the Freedom of Information Act 2000 may I kindly request the following information about your IT Infrastructure Information. The information needed is as follows:
SECURITY / CYBERSECURITY:

What SEIM (Security Event and Incident Management) solution is used by your organisation?
SolarWinds

When does your SEIM platform license subscription come up for renewal?
Renewal in March each year.

If the SEIM (Security Event and Incident Management) solution was purchased via third party, please disclose the contracting party's details?
We are unable to provide this information under article 43(2) of the Freedom of Information Act 2000 (Commercial Interests).

Do you outsource your security management to a third party (managed security service provider)? If so can you disclose the name of the managed security service provider.
NA

When does the current service contract from the current managed security service provider end?
NA

Can you provide the email address of the individual that is responsible for your IT Security?
it.marketing@secamb.nhs.uk

ICO - breaches:
How many cyber security breaches has your organisation had over the past 2 yrs?

The NHS 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 ICT infrastructure and would reveal details about the Trust's information security systems. The NHS Trust recognises that answering the request would promote openness and transparency with regards to the NHS 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 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 information security 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 ICT 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 ICT 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 ICT systems.

I hope you find this information of some assistance.

If for any reason you are dissatisfied with our response, kindly in the first instance contact Caroline Smart, Head of Information Governance via the following email address:

FOI@secamb.nhs.uk

Yours sincerely

Freedom of Information Coordinator
South East Coast Ambulance Service NHS Foundation Trust