Request for information under the Freedom of Information Act Reference 2021.839 Released 1 June 2021

Thank you for your email received 23 May 2021 requesting information regarding cyber-attacks.

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

Summary of your original request:
How many cyber-attacks (incidents) did your organisation experience in the last 3 years?

If these statistics are available within the cost limit, how many of those incidents involved a) Malware b) Ransomware c) Hacking d) Phishing emails

The Kent Community Health NHS Foundation Trust can neither confirm nor deny whether the information requested 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.

How many incidents over the last 3 years were reported to the Department of Health and Social Care, whether under the Security of Network and Information Systems Regulations 2018, or otherwise?

How many incidents over the last 3 years resulted in a notification to the Information Commissioner's Office?

How many incidents over the last 3 years were reported to both DHSC and the ICO?

Information relating to incidents reported to the ICO is readily available to the public by way of our annual reports which are published on our public website in September/October each year: https://www.kentcht.nhs.uk/about-us/our-aims/our-reports/.

This information is therefore exempt under Section 21 (2)(b) (information accessible to applicant by other means) and Section 22 (intended for further publication) of the Freedom of Information Act). The full wording of sections 21 and 22 can be found here:

Freedom of Information Act 2000 (legislation.gov.uk)

When reporting to the ICO, the information is automatically fed through to the Department of Health and Social Care.