NHS
Kirklees
Clinical Commissioning Group

Ref: 027FOI21.22 – Cyber Security

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
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?

Response

The CCG can neither confirm nor deny whether information is held under section 31(3) 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 CCG considers that to confirm or deny whether the requested information is held would indicate the prevalence of cyber- attacks against the CCG's ICT infrastructure and would reveal details about the CCG's information security systems. The CCG recognises that answering the request would promote openness and transparency with regards to the CCG'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 CCG, 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 CCG considers that confirming or denying whether the requested information is held would provide information about the CCG's information security systems and its resilience to cyber-attacks. There is a very strong public interest in preventing the CCG'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 CCG 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 CCG is able to detect and deal with ICT security attacks. The CCG'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 CCG's ICT systems. Disclosure of the information would assist a hacker in gaining valuable information as to the nature of the CCG'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 CCG being in a position where it would be more difficult to refuse 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 CCG's operations, including delivery of 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 CCG's ICT systems.

With regards to the reporting of incidents, you can find more information about that by reading the Corporate Governance Reports following this link: Annual reports (nkgh-ccg.co.uk). Please note that Kirklees CCG came into existence on 1 April 2021, and prior reports relate to our predecessor CCGs (Greater Huddersfield and North Kirklees). Please also note that information that is reasonably accessible by other means is exempt under section 21 of the Freedom of Information Act.