FOI 2122085 – Information Technology

NHS Calderdale CCG's response to your request can be found below.

1. **In the past three years has your organisation:**
    a. **Had any ransomware incidents? (An incident where an attacker attempted to, or successfully, encrypted a computing device within your organisation with the aim of extorting a payment or action in order to decrypt the device?) If yes, how many?**
    b. **Had any data rendered permanently inaccessible by a ransomware incident (i.e. some data was not able to be restored from back up.)**
    c. **Had any data rendered permanently inaccessible by a systems or equipment failure (i.e. some data was not able to be restored from back up.)**
    d. **Paid a ransom due to a ransomware incident / to obtain a decryption key or tool? If yes was the decryption successful, with all files recovered?**
    e. **Used a free decryption key or tool (e.g. from https://www.nomoreransom.org/)? If yes was the decryption successful, with all files recovered?**
    f. **Had a formal policy on ransomware payment? If yes please provide, or link, to all versions relevant to the 3 year period.**
    g. **Held meetings where policy on paying ransomware was discussed?**
    h. **Paid consultancy fees for malware, ransomware, or system intrusion investigation. If yes at what cost in each year?**
    i. **Used existing support contracts for malware, ransomware, or system intrusion investigation?**
    j. **Requested central government support for malware, ransomware, or system intrusion investigation?**
    k. **Paid for data recovery services. If yes at what cost in each year?**
    l. **Used existing contracts for data recovery services?**
    m. **Replaced IT infrastructure such as servers that have been compromised by malware? If yes at what cost in each year?**
    n. **Replaced IT endpoints such as PCs, Laptops, Mobile devices that have been compromised by malware?**
    o. **If yes at what cost in each year?**
    p. **Lost data due to portable electronic devices being mislaid, lost or destroyed? If yes how many incidents in each year?**

Calderdale CCG 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.

The CCG also has a legal requirement under part 3 section 10, (1, 2) of The Network and Information Systems Regulations 2018, to protect information about the security of our networks, we can't fulfil our requirements of the FOI if in doing so we breach NIS.

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 CCGs 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 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 CCGs information security systems and its resilience to cyber-attacks. There is a very strong public interest in preventing the CCGs 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 extend the CCG is able to detect and deal with ICT security attacks. The CCGs 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 CCGs ICT systems. Disclosure of the information would assist a hacker in gaining valuable information as to the nature of the CCGs 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 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 CCGs 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 CCGs ICT systems.

2. **Does your organisation use a cloud based office suite system such as Google Workspace (Formerly G Suite) or Microsoft’s Office 365?**

   Yes

   a. **If yes is this system’s data independently backed up, separately from that platform’s own tools?**

      Yes

3. **Is an offsite data back-up a system in place for the following? (Offsite backup is the replication of the data to a server which is separated geographically from the system’s normal operating location site.)**

a. **Mobile devices such as phones and tablet computers**

   Yes

b. **Desktop and laptop computers**

   Yes

c. **Virtual desktops**

   Yes

d. **Servers on premise**

   Yes

e. **Co-located or hosted servers**

   Yes

f. **Cloud hosted servers**

   Yes

g. **Virtual machines**

   Yes

h. **Data in SaaS applications**

   N/A

i. **ERP / finance system**

   Yes

j. **We do not use any offsite back-up systems**

   N/A

4. **Are the services in question 3 backed up by a single system or are multiple systems used?**

   The CCG uses multiple systems.

5. **Do you have a cloud migration strategy? If so is there specific budget allocated to this?**

   There is currently a cloud migration strategy under development for the CCG.

6. **How many Software as a Services (SaaS) applications are in place within your organisation?**

   The CCG has Five Software as a Service Applications

   a. **How many have been adopted since January 2020?**

No SaaS applications have been adopted since January 2020.