Hertfordshire Partnership University NHS Foundation Trust

20 September 2021

Information Rights & Compliance Team
99 Waverley Road
St Albans
Hertfordshire
AL3 5TL

Tel: 01727 804954
Email: Hpft.foi@nhs.net

Our Ref: FOI/04120

Thank you for your request concerning Ransomware And Data Back-Up.

Your request has been considered and processed in accordance with the requirements of the Freedom of Information (FOI) Act 2000.

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?)**
  - **i. 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?**
  - **i. 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/)?**
  - **i. If yes was the decryption successful, with all files recovered?**
  - **f. Had a formal policy on ransomware payment?**
  - **i. 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**
  - **i. 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?**
  - **i. 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?**
  - **i. If yes at what cost in each year?**
- **n. Replaced IT endpoints such as PCs, Laptops, Mobile devices that have been compromised by malware?**
  - **i. If yes at what cost in each year?**
- **o. Lost data due to portable electronic devices being mislaid, lost or destroyed?**
  - **i. If yes how many incidents in each year?**

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

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

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
b. Desktop and laptop computers
c. Virtual desktops
d. Servers on premise
e. Co-located or hosted servers
f. Cloud hosted servers
g. Virtual machines
h. Data in SaaS applications
i. ERP / finance system
j. We do not use any offsite back-up systems

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

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

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

a. How many have been adopted since January 2020?

The information you are requesting in question 1 to 6 are all relating to cyber security vulnerabilities and if answered could be used to compromise the security of the organisation. It would make the organisation vulnerable to a crime such as hacking and this could lead to a theft of information or a denial of service to IT systems therefore we have applied S31(1)(a) – Law Enforcement (1) Information is exempt if its disclosure under this Act world or would be likely to prejudice (a) the prevention or detection of crime.

S31 is subject to a test of prejudice. Please see below for our considered reasons for and against disclosure:

Reason in favour of disclosure

We acknowledge the public interest in openness and transparency and recognise that releasing this information would provide the public with assurance that we are protecting their information and our technologies.

Reason against disclosure

Disclosure of the use of certain ransomware incidents, operating systems and back up systems would make the Trust vulnerable to cybercrime as it outlines the Trust's security position which could be used as a starting point to attack network infrastructure and/or information systems.

We have reached the view that on balance, the public interest is better serviced by withholding this information under the section 31(1) exemption.

Should you require further clarification, please do not hesitate to contact me.

Please find enclosed an information sheet regarding copyright protection and the Trust's complaints procedure in the event that you are not satisfied with the response.

Yours sincerely

Sue Smith

Sue Smith
Information Rights Officer

Enc: Copyright Protection and Complaints Procedure Information Leaflet.

If you would like to complete a short survey in relation to your Freedom of Information request please scan the QR code below or click here.