Portsmouth Hospitals University NHS Trust

Freedom of Information Team
Post Room
Queen Alexandra Hospital
Southwick Hill Road
Portsmouth
Hampshire
PO6 3LY

Date: 30/09/2021
Ref: 21-22 291

Freedom of Information request

Thank you for your request for information under the Freedom of Information Act 2000, which was received by the Trust on 01/09/2021. Please see responses to your requests 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?)**
        i. **If yes, how many?** The Trust has had zero ransomware incidents.

    b. **Had any data rendered permanently inaccessible by a ransomware incident (i.e. some data was not able to be restored from back up.)**- Not applicable.

    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.)** No data has been rendered permanently inaccessible by a system or equipment failure.

    d. **Paid a ransom due to a ransomware incident / to obtain a decryption key or tool?** Not applicable.
        i. **If yes was the decryption successful, with all files recovered?** Not applicable.

    e. **Used a free decryption key or tool (e.g. from https://www.nomoreransom.org/)?** Not applicable.
        i. **If yes was the decryption successful, with all files recovered?** Not applicable

    f. **Had a formal policy on ransomware payment?**
    We are not obliged to provide information if its release would prejudice law enforcement. In this case, we believe that releasing detailed information such as IT security and resilience arrangements creates a security risk and is likely to prejudice the prevention or detection of crime (section 31(1)(a) and the administration of justice (section 31(1)(c)).

    In line with the terms of this exemption in the Freedom of Information Act, we have also considered whether it would be in the public interest for us to provide you with the information, despite the exemption being applicable. In this case, we have concluded that the public interest favours withholding the information.

You can find out more about Section 31 by reading the extract from the Act and some guidance points we consider when applying this exemption, attached at the end of this letter.

You can also find more information by reading the full text of the Act, http://www.legislation.gov.uk/ukpga/2000/36/section/31 and further guidance

When assessing whether or not it was in the public interest to disclose the information to you, we considered the following factors:

Public interest considerations favouring disclosure

- There is public interest in transparency and accountability of the Trust.
- Disclosure may promote public understanding.
- There is public interest in good decision-making by public bodies.

Public interest considerations favouring withholding the information

Disclosing details of IT security and resilience arrangements that the Trust considers will put it at risk from criminal and malicious activity and prejudice its ability to resist cyber-attacks and similar.

We reached the view that, on balance, the public interest is better served by withholding this information under Section 31(1)(a) and (b) of the Act at this time.

i. **If yes please provide, or link, to all versions relevant to the 3 year period.** Not applicable.

g. **Held meetings where policy on paying ransomware was discussed?** Please see answer in question 1 (f).

h. **Paid consultancy fees for malware, ransomware, or system intrusion investigation**
   i. **If yes at what cost in each year?** The Trust has spent £2550 excluding VAT in 2019.

i. **Used existing support contracts for malware, ransomware, or system intrusion investigation?** The Trust has not used any of the above systems.

j. **Requested central government support for malware, ransomware, or system intrusion investigation?** The Trust has not requested any central government support

k. **Paid for data recovery services?** The Trust has not paid for a data recovery service.
   i. **If yes at what cost in each year?** Not applicable

l. **Used existing contracts for data recovery services?** The Trust has not used existing contracts for data recovery services.

m. **Replaced IT infrastructure such as servers that have been compromised by malware?** The Trust has not replaced any infrastructure that has been compromised by malware.
   i. **If yes at what cost in each year?** Not applicable.

n. **Replaced IT endpoints such as PCs, Laptops, Mobile devices that have been compromised by malware?** The Trust has not replaced any of the above devices that have been compromised by malware.
   i. **If yes at what cost in each year?** Not applicable.

o. **Lost data due to portable electronic devices being mislaid, lost or destroyed?**
    i. **If yes how many incidents in each year?**

The Trust is not able to readily retrieve this information and therefore to undertake this would require a manual search process which would exceed 18 hours. Therefore, this would exceed the appropriate limit for dealing with a Freedom of Information Request, in terms of costs and therefore Section 12(1) of the Freedom of Information Act 2000 applies.

2. **Does your organisation use a cloud based office suite system such as Google Workspace (Formerly G Suite) or Microsoft's Office 365?** The Trust uses Microsoft Office 365.
    a. **If yes is this system's data independently backed up, separately from that platform's own tools?** Please see answer in question 1 (f).

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**

    Please see answer in question 1 (f).
4. **Are the services in question 3 backed up by a single system or are multiple systems used?** Please see answer in question 1 (f).

5. **Do you have a cloud migration strategy? If so is there specific budget allocated to this?** The Trust follows the NHS strategy for migration to the cloud. There is no dedicated budget allocated, expenditure is included within wider budgets/allocations.

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 Trust is not able to readily retrieve this information and therefore to undertake this would require a manual search process which would exceed 18 hours. Therefore, this would exceed the appropriate limit for dealing with a Freedom of Information Request, in terms of costs and therefore Section 12(1) of the Freedom of Information Act 2000 applies.

Please accept this letter as completion of your request. Please note that copies of this request will be held on file for three years before being confidentially destroyed.

If you are dissatisfied with the outcome of your request, please contact our Head of Information Governance on Information.Governance@porthosp.nhs.uk or write to the above address and we will conduct an internal review. Upon review, if you are still dissatisfied, you may appeal our decision by contacting the Information Commissioner's Office; for more information, please visit the ICO's website.

Please be aware, if we do not receive an appeal within 30 days of you receiving this letter, we will assume that you are satisfied with our response. If you have any further queries, please do not hesitate to contact us.

Yours sincerely

Freedom of Information Team