Portsmouth Hospitals University NHS Trust

Freedom of Information Team
De La Court House
Queen Alexandra Hospital
Southwick Hill Road
Portsmouth
Hampshire
PO6 3LY

Name:
Email:
Date: 13/07/2023
Ref: 23-24 159

Dear

RE: 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 09/06/2023. Please see responses to your requests below.

1. **What software/tools/products do you currently have in place to securely: manage privileged user access/administrator accounts/manage endpoints.**
   The Trust uses industry standard tooling and software provided by Microsoft and NHS England.

   The Trust is 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)).

2. **How do you comply with the DSPT requirements surrounding privileged access/managing administrator accounts?**
   The Trust complies with DSPT requirement for managing privileged access by demonstrating compliance with DSPT 4.4.1 and 4.4.2. This is achieved using standard controls such as Microsoft Privileged Identity Management and security activity log archiving.

3. **How many data breaches/data security incidents have you suffered as a result of accidental or deliberate misuse of access credentials in the last 3 years? Please break these down year by year. (*A data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data).**
   Please see table below. These relate to the misuse of legitimate access to clinical systems from staff looking up personal information of patients, which were not related to their work.

2020/2021	2021/2022	2022/2023
9	6	6

4. **When carrying out and completing DSPT assessments, do you have a dedicated employee/s for this, and can you specify the job title/s of those responsible, how long does it take, and how many staff are involved?**

The DSPT is a collaboration between the Information Governance Team and the IT Security Team. The DSPT is managed by the Senior IG Officer and the Head of IG. Major contributors include the Head of Cyber Security, Clinical Coding Manager, Emergency Planning and Resilience Manager, Workforce and Transformation Manager, Deputy Chief Information Officer, and Head of Legal & Compliance (Procurement). Evidence is gathered for the DSPT over 10 months after the new version is released.

5. **How beneficial and efficient do you think DSPT assessments are as a means of assessing data security best practice?**
   This is asking for an opinion; therefore, we are not required to answer this. The Trust has decided that it would not be helpful to you for us to answer your request under the FOIA as it does not qualify as a valid Freedom of Information request. The Act covers any recorded information that is held by a public authority. For example, recorded information includes printed documents, computer files, letters, emails, photographs, and sound or video recordings, therefore public authorities can refuse to answer any requests that are asking for statements or opinions

6. **What actions are you taking to ensure your organisation complies with the new NHS Cyber Strategy?**
   The organisation is currently reviewing the new guidance with NHS England and liaising with the Future NHS Cyber Associates Network to ensure local policies align to the new NHS Cyber strategy.

7. **What security tech/software/tools does your organisation use to help you comply with DSPT and cyber resilience in general? For example, MFA, email filtering, Privileged Access Management, Anti-Virus, back-up protection, endpoint management**
   Please see exemption in Question 1.

8. **Do you keep an accurate log of who has privileged user access to each, IT system, device, application and database – including third party suppliers - and how do you manage this?**
   This is achieved using standard controls such as Microsoft Privileged Identity Management and security activity log archiving. Access by third-party suppliers is managed by individual remote access agreements.

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