University Hospitals Bristol NHS
NHS Foundation Trust

Freedom of Information Request **Ref: UHB 17-620**

Date 14 December 2017

[redacted]

Thank you for your request for information under the Freedom of Information Act 2000. The Trusts response is as follows:

1. **As the data controller how do you maintain control over a personal device opposed to a corporately owned and provided device?**
   Both are controlled with our Master Data Management (MDM) product.

2. **What type of data is held on personal devices?**
   Emails and Calendar appointments are held on personal devices.

3. **Where may data be stored on personal devices?**
   The Trust permits data on personal devices to be store only on the device itself and in an encrypted format.

4. **How is data transferred to and from the device?**
   The Trust transfers data to and from devices via encrypted means.

5. **How do you protect the data transfer from personal devices so as not to infect the corporate network from threats?**
   The Trust protects the data transfer from personal devices so as not to infect the corporate network from threats with our MDM product.

6. **How do you protect against data leakage from the device or application?**
   The Trust protects against data leakage from the device or application with our MDM product.

7. **How do you deal with the blurring of personal and business use on personal devices?**
   The Trust deals with the blurring of personal and business use on personal devices with our MDM product

8. **What are the minimum device security capacities required to connect to your corporate or clinical network?**
   The minimum device security capacities required to connect to the Trust's corporate/clinical network is that all devices must be running the latest operating system version.

9. **Do you support staff personal devices when connected to your network?**
   Yes

10. **Who supports personal devices when connected to your network?**
    The Trust's IT Department supports personal devices when connected to our network.

11. **What management, standards, polices and/or SLAs' are placed around the management of personal devices and their support?**
    We do hold the requested information however we are unable to disclose under Section 31(1)(a) of the Freedom of Information Act it as we have considered disclosure of the information would, or would be likely to, prejudice the prevention or detection of crime. Under guidance issued by the Information Commissioner states that this exemption applies if disclosure of the withheld information would, or would be likely to prejudice the prevention of criminal acts in relation to the Trust's computer systems and information, such as hacking, theft of data, misuse of confidential data or the disruption of the Trust's operations.

12. **What process do staff follow when the person who owns the device leaves their employment?**
    The Trust remotely removes any work related data from the device when a staff member leaves their employment.

13. **How do you deal with the loss, theft, failure and support of personal devices?**
    The Trust wipes lost devices and the IT Department support the function of work information on personal devices

14. **What technology or technologies underpin your personal device (BYOD) capabilities (This should list all the technologies used to provide, secure and manage the devices/service)?**
    The Trust's MDM product underpins our personal device capabilities.

15. **May I please ask you to send me any of the following polices, or others that are applicable to your Trust's BYOD (or equivalent) policy/capabilities.**
    - **Information Security Policy**
    - **Internet Policy**
    - **Email policy**
    - **Anti-virus Policy**
    - **Network & Remote Access Security Policies**
    - **Bring Your Own Device (BYOD) or personal device Policy**

    We do hold the requested information however we are unable to disclose under Section 31(1)(a) of the Freedom of Information Act it as we have considered disclosure of the information would, or would be likely to, prejudice the prevention or detection of crime. Under guidance issued by the Information Commissioner states that this exemption applies if disclosure of the withheld information would, or would be likely to prejudice the prevention of criminal acts in relation to the Trust's computer systems and information, such as hacking, theft of data, misuse of confidential data or the disruption of the Trust's operations.

Public interest arguments in favour of disclosing the withheld information.

The Trust is aware of the presumption of openness and transparency running through the Freedom of Information Act, and that public authorities should be accountable to the public for their actions and decision-making processes, as public funds are involved.

The Trust also considers that there is a public interest in knowing that it manages data responsibly and securely.

Public interest factors in favour of maintaining the exemption

The Trust believes that the public interest arguments in favour of withholding the small amount of information are compelling. There is a strong public interest in the highest standards of information compliance being maintained in all public sector organisations; and in particular the secure maintenance of personal and other sensitive data. The Trust considers that disclosure of the information would be likely to prejudice the maintenance of its IT security is clearly contrary to the public interest.

Balance of the public interest arguments

The Trust considers that there is a strong public interest in openness and transparency of public authorities. There would be a significant public interest in knowing that the Trust manages data responsibly and securely, particularly since it holds a great deal of confidential and valuable data.

The Trust does not believe that there is any compelling public interest in knowing the details of our Cyber Security policies as these are potentially vulnerable to our software applications, which would outweigh the public interest in the Trust's secure maintenance of sensitive and confidential data. University Hospitals Bristol NHS Trust accepts that there is a strong public interest in maintaining the security of confidential data and not increasing the vulnerably of the security systems to criminal activity.

The Trust has carefully considered all public interest arguments both in favour of disclosure and of maintaining the exemption. We have considered that it is vitally important to protect the security of our IT systems against criminal or malicious attack and that there is an extremely compelling interest in doing so. We do not believe that this is outweighed by the arguments in favour of openness and transparency in public sector organisations.

The Trust considers that the public interest in maintaining the exemption in all of the circumstances of this case outweighs that in disclosure of the withheld information. Under guidance from the Freedom of Information Act, the Trust has therefore decided to withhold the requested information.

This concludes our response. We trust that you find this helpful, but please do not hesitate to contact us directly if we can be of any further assistance.

If, after that, you are dissatisfied with the handling of your request, you have the right to ask for an internal review. Internal review requests should be submitted within two months of the date of receipt of the response to your original letter and should be addressed to:

Trust Secretary
University Hospitals Bristol NHS Foundation Trust
Trust Headquarters
Marlborough Street
Bristol
BS1 3NU

Please remember to quote the reference number above in any future communications.

If you are not content with the outcome of the internal review, you have the right to apply directly to the Information Commissioner for a decision. The Information Commissioner can be contacted at: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

To view the Freedom of Information Act in full please click here.

Yours sincerely,

[redacted]