University Hospitals Bristol NHS
NHS Foundation Trust

Freedom of Information Request **Ref: UHB 17-579**

Date 26 January 2018

By Email

[redacted]

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

I am carrying out some research relating to the level of security currently used by NHS Trusts on mobile device estates. Please could I ask you to respond to this Freedom of Information request on behalf of your Trust?

1/	**Are your mobile devices enabled for corporate email?**	No
	If you answered No to Question 1, please move straight to Question 3	
2/	**Is corporate email delivered to your devices purely using Microsoft Exchange ActiveSync (with no other Mobile Device Management solution used)?**	No
	If you answered Yes to Question 2, please move straight to Question 6	
3/	**Which Mobile Device Management solution(s) do you use?**	Under **Section 31(1)(a)** of the Freedom of Information Act, we are required to judge as to whether the 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.
4/	**How many MDM licences do you currently have?**	1500
5/	**When are your Mobile Device Management licences valid until?**	Ongoing
6/	**If a user accidentally breaks their mobile device, how many days does it currently take to get a fully working replacement device to them?**	2 days

7/	**Do you manage your MDM solution in-house or use a third party managed service?**	In house
8/	**If third party managed, which organisation manages your Mobile Device Management solution for you?**	Not applicable
9/	**Do you use any form of Endpoint Threat Prevention on your mobile devices to flag potential cyber risks proactively?**	Yes
	If you answered No to Question 9, please move straight to Question 14	
10/	**Which Endpoint Threat Prevention solution(s) do you use?**	**Under Section 31(1)(a)** of the Freedom of Information Act, we are required to judge as to whether the 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.
11/	**If you use Endpoint Threat Prevention solution(s), which of these security risks are detected:**	
	Distributed Denial of Service	Yes
	Suspicious Domain	Yes
	Digital Identity Monitoring	Yes
	Information Leaks	Yes
	Credential Theft	Yes
	Phishing	Yes
	Malware	Yes
	Suspicious Mobile Apps	Yes
12/	**How many endpoint threat protection licences do you have?**	1500
13/	**When are your Endpoint Threat Protection licences valid until?**	Ongoing
14/	**Do you allow mobile devices to connect to your corporate network that are more than 2 full releases behind the latest version of the operating system software?**	No
15/	**Are you currently able to restrict access to certain websites across your entire mobile device estate?**	Yes
16/	**If you need to wipe corporate data off a mobile device, what means do you use to wipe a device, either remotely or in hand?**	Remotely
17/	**Is the data wipe auditable?**	Yes

18/	**Are you currently operating your mobile devices in compliance with the General Data Protection Regulation (GDPR), enforceable from May 2018?**	Yes
19/	**How do you currently dispose of a device which is no longer to be used?**	Wiped then recycled
20/	**Is your device disposal fully auditable?**	Yes

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 Mobile Device Management solution(s) or Which Endpoint Threat Prevention solution(s) we use as these are potentially vulnerable 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]