Skipton House
80 London Road
London SE1 6LH

T: 020 3747 0000
E: nhsi.enquiries@nhs.net
W: improvement.nhs.uk

23 July 2020

[redacted]
By email
[redacted]

Dear [redacted]

Request under the Freedom of Information Act 2000 (the "FOI Act")

We refer to your email of 28 February 2020 in which you requested information under the FOI Act from NHS Improvement. Since 1 April 2016, Monitor and the NHS Trust Development Authority have been operating as an integrated organisation known as NHS Improvement. For the purposes of this decision, NHS Improvement means Monitor and the TDA.

Your request

The full terms of your request has been annexed.

Decision

NHS Improvement holds some of the information you have requested and has decided to release some of the information it holds. Some of the information is being withheld under section 31 of the FOI Act.

1. **Are the Data Centre's operated by or for the organisation fit for purpose? For example, is there a Business Continuity Plan, is there Disaster Recovery in place or is it a single site?**

   Yes (and migrating to Crown Hosting)

2. **Is there any capital investment in data centres planned in the next 36 months? For example, Mechanical & Electrical or refresh of equipment within the DC such as network, storage area network?**

   No, please see the response to question 1

3. **Is data privacy and or information security compliance a priority for the organisation's board?**

Yes

4. On your Organisation's risk register, are there any Information Technology related risks?

Yes

i) If time/ cost allows, please list the top three related risks.

We are able to list some of our risks which relate to information technology as follows:

- Cyber Security Risk: Targeted Phishing Emails - There is a risk that phishing emails that are targeted at certain members of staff could be difficult to identify and could result in compromises to accounts and our network.
- Malicious code including Ransomware - There is a risk that Ransomware or other malicious code could be installed to our organisations devices. This will result in our devices being compromised and data potentially being extracted, deleted, altered or encrypted on a large scale without recovery.

We confirm our Cyber Risks register currently holds another 7 cyber security vulnerabilities relating to information technology, but are withholding this information under section 31 of the FOI Act.

Section 31(1)(a) provides an exemption from the right to know if disclosure would, or would be likely to, prejudice the prevention or detection of crime.

We consider listing all of our cyber security vulnerabilities would be likely to leave NHS Improvement more vulnerable to targeted, malicious attacks on our cyber security systems. Hackers could use this information to their advantage to compromise our computer systems as such we consider withholding this information would be likely to prevent criminal activity.

We have considered the general public interest test in openness and transparency with regards to how public authorities use their resources and identify potential risks within its organisation. However, we consider there is an overwhelming public interest in keeping the information held by NHS Improvement (which includes patient identifiable data) within its computer systems securely. We have therefore concluded the public interest is best served by withholding this information.

5. Are the cyber security vulnerabilities within the organisation's existing Information Technology estate increasing?

We cannot quantify this due to the variance of vulnerabilities and automated vulnerability patching and controls which are in place internally and through third parties (this includes auto patching by the likes of Microsoft etc.)

i) Has the organisation had a security breach in the past 12 months?

No (where breach is defined as a third party maliciously circumnavigating or breaching our security controls to access the organisations information or assets)

6. **Did the organisation meet its Information Technology savings target in the last Financial Year?**

   Yes

7. **What percentage of Information Technology budget is currently allocated to "on-premises" capability vs "cloud" capability?**

   Once the move to crown Hosting is completed we will be deemed to be 100% based in the Cloud.

8. **Does the organisation have the skills and resource levels necessary for moving to the cloud?**

   Yes

9. **What percentage of the Information Technology department headcount are software developers?**

   Our Corporate Information Technology department does not employ anyone who has 'software developer' as their job title. There are numerous 'developer' related roles across the organisation in various teams but we do not hold a central database for headcount due to the varying roles and job descriptions.

10. **In relation to contracts with Amazon Web Services, Microsoft for Azure and/or Google for Google Cloud, was the monthly expenditure higher than budgeted?**

    No – in line with expectations

    i) **If yes, has the organisation been able to subsequently reduce the cost whilst maintaining service levels for users?**

       N/A

Review rights

If you consider that your request for information has not been properly handled or if you are otherwise dissatisfied with the outcome of your request, you can try to resolve this informally with the person who dealt with your request. If you remain dissatisfied, you may seek an internal review within NHS Improvement of the issue or the decision. A senior member of NHS Improvement's staff, who has not previously been involved with your request, will undertake that review.

If you are dissatisfied with the outcome of any internal review, you may complain to the Information Commissioner for a decision on whether your request for information has been dealt with in accordance with the FOI Act.

A request for an internal review should be submitted in writing to FOI Request Reviews, NHS Improvement, Skipton House, 80 London Road, London SE1 6LH or by email to nhsi.foi@nhs.net.

Publication

Please note that this letter will shortly be published on our website. This is because information disclosed in accordance with the FOI Act is disclosed to the public at large. We will, of course, remove your personal information (e.g. your name and contact details) from the version of the letter published on our website to protect your personal information from general disclosure.

Yours sincerely,

NHS Improvement

Annex – FOI request

Under the Freedom of Information Act 2000 I seek the following information:

1. Are the Data Centre's operated by or for the organisation fit for purpose? For example, is there a Business Continuity Plan, is there Disaster Recovery in place or is it a single site?
2. Is there any capital investment in data centres planned in the next 36 months? For example, Mechanical & Electrical or refresh of equipment within the DC such as network, storage area network?
3. Is data privacy and or information security compliance a priority for the organisation's board?
4. On your Organisation's risk register, are there any Information Technology related risks?

i) If time/ cost allows, please list the top three related risks.

5. Are the cyber security vulnerabilities within the organisation's existing Information Technology estate increasing?

i) Has the organisation had a security breach in the past 12 months?

6. Did the organisation meet its Information Technology savings target in the last Financial Year?
7. What percentage of Information Technology budget is currently allocated to "on-premises" capability vs "cloud" capability?
8. Does the organisation have the skills and resource levels necessary for moving to the cloud?
9. What percentage of the Information Technology department headcount are software developers?
10. In relation to contracts with Amazon Web Services, Microsoft for Azure and/or Google for Google Cloud, was the monthly expenditure higher than budgeted?

i) If yes, has the organisation been able to subsequently reduce the cost whilst maintaining service levels for users?

I would prefer to receive this information electronically, preferably as a data set, e.g. in Excel, NOT as a PDF. If the decision is made to withhold some of this data using exemptions in the Data Protection Act, please inform me of that fact and cite the exemptions used.

If some parts of this request are easier to answer than others, I would ask that you release the available data as soon as possible. If you need any clarification then please do not hesitate to contact me. Under Section 16 it is your duty to provide advice and assistance and so I would expect you to contact me if you find this request unmanageable in any way. I would be grateful if you could confirm in writing that you have received this request, and I look forward to hearing from you within the 20-working day statutory time period.