Freedom of Information Act 2000 (FOIA)
Decision notice

Date: 17 May 2022

Public Authority: University College London Hospitals NHS Foundation Trust

Address: 2nd Floor Maple House
149 Tottenham Court
London W1T 7NF

Decision (including any steps ordered)

1. The complainant has requested information relating to a number of University College London Hospitals NHS Foundation Trust (UCLH) policies.

2. UCLH provided all the information requested aside from the Information Security Policy.

3. The Commissioner's decision is that UCLH is entitled to rely on section 31(1)(a) to withhold the information relating to the Information Security Policy.

4. The Commissioner does not require UCLH to take any steps as a result of this decision notice.

Request and response

5. On 11 June 2021, the complainant wrote to UCLH and requested information in the following terms:

"The document provided makes reference to other documents it is to be read in conjunction with…can I request the following documents as referenced on the cover page:

- *Information Risk Policy*
- *Data Protection Confidentiality Policy*
- *Information Security Policy*

- *Incident Reporting Policy*
- *Records Management Policy*
- *Freedom of Information Act Policy*
- *Disciplinary Policy and Procedure"*

6. UCLH responded on 8 July 2021 and provided all the requested information aside from the Information Security policy, which it advised would follow.

7. The complainant requested an internal review on 15 July 2021 as the policy remained outstanding. On 24 August 2021 UCLH provided a copy of the policy, however it stated that some information was exempt under section 31 FOIA.

8. The complainant did not request an internal review of the application of section 31. However, given the time elapsed since the request and complaint to the Commissioner, the Commissioner exercised his discretion, accepted the case and wrote to UCLH accordingly.

Scope of the case

9. The complainant contacted the Commissioner on 23 September 2021 to complain about the way their request for information had been handled and stated:

"I would draw the ICO's attention to the fact that NHS England the body that the UCLH Hospital Trust is ultimately governed under publishes its own version of the document requested as do many other hospitals in the UK, examples of which are shown below:

information-security-policy-v4.0.pdf.england.nhs.uk
http://www.shropscommunityhealth.nhs.uk/content/doclib/10420.pdf
https://www.fhft.nhs.uk/media/4234/information-security-policy.pdf
https://doclibrary-rcht.cornwall.nhs.uk/DocumentsLibrary/RoyalCornwallHospitalsTrust/HealthInformatics/InfrastructureTechnicalSecurity/InformationSecurityPolicy.pdf
https://www.gwh.nhs.uk/media/327830/security-policy.pdf
https://www.enhertsccg.nhs.uk/sites/default/files/documents/Jan2017/Information-Security-Policy-9.1.1-%20ENHCCG.pdf

On this basis I contest the argument put forward to redact sections to the extent they have been as clearly comparable organisations and the

ultimate NHS body in England take a view that is inconsistent with the response provided in the internal review."

10. The Commissioner considers the scope of this case to be to determine if UCLH is entitled to rely on section 31 to withhold part of the requested information (the withheld information).

Reasons for decision

Section 31 – law enforcement

11. UCLH has argued that the withheld information is exempt on the basis of section 31(1)(a) – the prevention and detection of crime, and 31(1)(g) which provides that information is exempt if its disclosure would or would be likely to prejudice the exercise by any public authority of the functions in section 31(2) of the FOIA. Section 31 can be claimed by any public authority, not just those with law enforcement functions.

12. Section 31(1)(a) states:

"(1) Information which is not exempt information by virtue of section 30 is exempt information if its disclosure under this Act would, or would be likely to, prejudice— (a) the prevention or detection of crime,'

13. UCLH explained that the appendices redacted from the Information Security policy have been undertaken on the basis of section 31(1)(a). It considered having access to this information would allow potential perpetrators to commit cybercrimes against this NHS trust, which might involve the theft of staff/patient confidential information, financial fraud, blackmail and denial of systems critical to the treatment of patients, such as the WannaCry ransomware attack in 2017 that prevented multiple Trusts from accessing critical systems for weeks[1].

14. UCLH provided the Commissioner with a number of examples from the redacted appendices of the policy which illustrate how this information could be utilised by cybercriminals to bypass its network security measures. Clearly it is not appropriate to detail them here. However, it relates to technical security policies, operational security policies and security management policies.

[1] https://www.bbc.co.uk/news/health-39899646

Is the exemption engaged?

15. In order for a prejudice based exemption such as that contained within section 31(1)(a) to be engaged, the Commissioner considers that three criteria must be met.

    - Firstly, the actual harm which the public authority alleges would, or would be likely, to occur if the withheld information was disclosed has to relate to the applicable interests within the relevant exemption;

    - Secondly, the public authority must be able to demonstrate that some causal relationship exists between the potential disclosure of the information being withheld and the prejudice which the exemption is designed to protect. Furthermore, the resultant prejudice which is alleged must be real, actual or of substance; and

    - Thirdly, it is necessary to establish whether the level of likelihood of prejudice being relied upon by the public authority is met – ie, disclosure 'would be likely' to result in prejudice or disclosure 'would' result in prejudice. In relation to the lower threshold the Commissioner considers that the chance of prejudice occurring must be more than a hypothetical possibility; rather there must be a real and significant risk. With relation to the higher threshold, in the Commissioner's view this places a stronger evidential burden on the public authority. The anticipated prejudice must be more likely than not.

16. With regard to the first criterion of the three limb test described above, the Commissioner accepts that the potential prejudice described by the public authority generally relates to the interests which the exemption contained at section 31(1)(a) is designed to protect. Specifically, disclosing this sort of information would provide potential cyber criminals to gain access to UCLH's network allowing it to 'harvest' information including personal data, as well as financial systems.

17. Having viewed the withheld information and considered the examples provided, the Commissioner is satisfied that the prejudice alleged by UCLH is real and of substance, and is prepared to accept that there is a causal relationship between the disclosure of the requested information and an increased risk to UCHL of being targeted.

18. He must however establish whether disclosure would be likely to result in the prejudice alleged (ie the third criterion).

19. UCLH considered the likelihood of harm occurring is high as NHS Trusts have been subject to repeated cyberattacks such as the WannaCry ransomware attack referred to above. In its annual review, published on 3 November 2021, the National Cyber Security Centre reported on its handling of 723 cyber security incidents between 1 September 2019 and

31 August 2020, with particular focus on bolstering the NHS in the wake of the pandemic. More than 160 "high-risk and critical vulnerabilities" were shared with NHS trusts to raise awareness of threats.[2]

20. It is difficult to prove something that may happen in future if the information were disclosed and the Commissioner is of the view that UCLH cannot demonstrate that disclosure 'would' result in prejudice. However, in the case of *John Connor Press Associates Limited v The Information Commissioner (EA/2005/0005)* the Tribunal confirmed that, when determining whether prejudice would be likely, the test to apply is that "*the chance of prejudice being suffered should be more than a hypothetical possibility; there must have been a real and significant risk".* (paragraph 15). In other words, the risk of prejudice need not be more likely than not, but must be substantially more than remote. The Commissioner accepts that disclosure of the withheld information would be likely to prejudice the prevention of crime.

21. The Commissioner accepts that disclosing the withheld information 'would be likely' to pose a real and significant risk of prejudice to the prevention or detection of crime.

22. The Commissioner finds that the prejudice test has been satisfied in the circumstances of this case and consequently the exemption at section 31(1)(a) is engaged.

23. Section 31 is a qualified exemption. By virtue of section 2(2)(b) of the Act, UCLH can only rely on section 31 as a basis for withholding the information in question if the public interest in doing so outweighs the public interest in disclosure.

Public interest test

24. The complainant has not made any submissions with regard to the public interest test.

25. UCLH acknowledge there is a public interest in understanding that public authorities are adopting policy guidance and have controls, and general countermeasures in place.

26. On the other hand there is a public interest in enabling public authorities to carry out their business without opening themselves up to unnecessary risk through disclosure of information which would reveal vulnerabilities or weaknesses in their systems.

[2] NHS withstands hundreds of cyber crime incidents relating to Covid-19 (digitalhealth.net)

27. Disclosure of the information requested would reveal situations where UCLH's countermeasures are potentially vulnerable to further attacks.

28. UCLH has a duty to assist those providing it with law enforcement capabilities. This includes those protecting its information technology services and infrastructure from malicious activity, especially targeted attacks.

29. Disclosure of more detailed information on countermeasures would prejudice UCLH's ability to support those providing it with law enforcement capabilities, encouraging those with malicious intent towards UCLH to target its systems thereby increasing the challenges they face in enforcing the law.

30. It therefore considered that the public interest in withholding the information outweighs that of disclosure.

Balance of the public interest arguments

31. The Commissioner considers that there is always some public interest in the disclosure of information. This is because it promotes the aims of transparency and accountability, which in turn promotes greater public engagement and understanding of the decisions taken by public authorities. He accepts there will be a public interest in information which shows how the NHS are dealing with cyber-attacks ensuring robust IT systems are in place.

32. The Commissioner has taken account of the complainant's argument that NHS England publishes its own version of the document as do many other hospitals in the UK. However, it should be noted that each request is dealt with on its own merits and is subject to each public authorities assessment of risk. Furthermore, it is possible that the withheld information in this case is different to that disclosed by NHS England.

33. In addition, the Commissioner noted that UCLH's systems holds the personal data of hundreds of members of staff along with the sensitive personal data of hundreds of patients. There is, therefore, a strong public interest in protecting this personal data from unlawful access as well as a strong public interest in ensuring that UCLH's is not hacked and patient care interfered with.

34. Taking all of this into account the Commissioner considers that the public interest in favour of disclosure does not carry much weight beyond that in transparency of its processes.

35. In contrast, there is a strong and compelling argument for maintaining the exemption to preserve UCLH's ability to effectively deliver patient care and maintain the safety and welfare of its staff and patients.

36. In the specific circumstances of this case, the Commissioner considers that the public interest in maintaining the exemption outweighs that in disclosure.

Right of appeal

37. Either party has the right to appeal against this decision notice to the First-tier Tribunal (Information Rights). Information about the appeals process may be obtained from:

    First-tier Tribunal (Information Rights)
    GRC & GRP Tribunals,
    PO Box 9300,
    LEICESTER,
    LE1 8DJ

    Tel: 0300 1234504
    Fax: 0870 739 5836
    Email: grc@justice.gov.uk
    Website: www.justice.gov.uk/tribunals/general-regulatory-chamber

38. If you wish to appeal against a decision notice, you can obtain information on how to appeal along with the relevant forms from the Information Tribunal website.

39. Any Notice of Appeal should be served on the Tribunal within 28 (calendar) days of the date on which this decision notice is sent.

Signed .....

Susan Duffy
Senior Case Officer
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF