Freedom of Information Act 2000 (FOIA)

Decision notice

Date: 10 August 2017

Public Authority: Northern Lincolnshire and Goole NHS Foundation Trust

Address: Diana, Princess of Wales Hospital
Scartho Road
Grimsby
North East Lincolnshire
DN33 2BA

Decision (including any steps ordered)

1. The complainant has requested a copy of a report into a cyber-incident at Northern Lincolnshire and Goole NHS Foundation Trust ("the Trust"). The Trust refused the request on the basis of section 31 of the FOIA and later sought to also rely on 36(2)(c).

2. The Commissioner's decision is that the Trust has correctly applied the provisions at section 31(1)(a) and (b) of the FOIA and the public interest favours withholding the information in the NCC report. The Commissioner does not require any steps to be taken.

Request and response

3. On 30 January 2017, the complainant wrote to the Trust and requested information in the following terms:

"I am requesting a full copy of the NCC report into the cyber-incident at Northern Lincolnshire and Goole, as referenced in the January 2017 board papers here - http://www.nlg.nhs.uk/content/uploads/2016/12/NLG17044-Resources-Committee-Minutes-public.pdf "

4. The Trust responded on 14 February 2017. It stated that as the police cyber-crime unit was still investigating the incident it could prejudice the investigation to publish the NCC report and the information was therefore being withheld under section 31 of the FOIA.

5. Following an internal review the Trust wrote to the complainant on 13 March 2017. It stated that it maintained the information should be withheld due to the ongoing police investigation. It clarified it was relying on section 31(1)(a) of the FOIA and outlined the public interest arguments it had considered.

Scope of the case

6. The complainant contacted the Commissioner on 14 March 2017 to complain about the way her request for information had been handled.

7. During the course of her investigation the Trust clarified it was relying on section 31(1)(a), 31(1)(b) and 31(1)(g) with 31(2)(a). As well as the various subsections of section 31 the Trust considered relevant it also sought to apply the exemption at section 36(2)(c).

8. The Commissioner considers the scope of her investigation to be to determine if the Trust is entitled to rely on any of the sub-sections of section 31 or section 36(2)(c) to withhold the NCC report.

Reasons for decision

Section 31 – law enforcement

9. Section 31(1) states that:

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,

(b) the apprehension or prosecution of offenders,

(g) the exercise by any public authority of its functions for any of the purposes specified in subsection (2),

10. Section 31(2) states that:

The purposes referred to in subsection (1)(g) to (i) are –

(a) the purpose of ascertaining whether any person has failed to comply with the law,

11. In determining whether prejudice would or would be likely to occur from disclosure, the Commissioner will consider the nature and likelihood of the prejudice in question occurring.

12. The Trust has clarified it is seeking to rely on section 31 on the basis of the prejudice to the police's functions. The Trust has explained that the NCC report is key evidence for the police in their investigation and the Trust has provided evidence it has been in contact with the police regarding possible disclosure of the report and they have objected in very strong terms to this. It is considered that disclosure would prejudice the ongoing police investigations into the cyber-attack and therefore the police's functions under section 31(1)(a) and (b). Further information on exactly how the information in the NCC report would have this prejudicial effect is provided in a confidential annex to this decision notice provided to the Trust.

13. The Commissioner has to consider not just whether the section 31 exemption can be engaged but whether it is engaged in this case and where the balance of the public interest lies.

14. The police have advised the Trust to restrict circulation and publication of the report as it would provide the perpetrator of the attack with information that the police is using to track them, assisting them to evade capture and prosecution. The detail of the report is discussed in the confidential annex and the Commissioner, having viewed this information is clear that the NCC report contains a very detailed account of the attack including the route of hacking used and the methods being used by the police to track the perpetrator.

15. The Trust has argued that disclosure of the NCC report 'would' prejudice ongoing police investigations into the cyber-attack to apprehend offenders and therefore the functions set out in section 31(1)(a) and (b). This means the likelihood of the prejudice occurring should be more probable than not.

16. The Commissioner accepts that the detail of the NCC report is such that disclosure of the report would impact on the police's investigation and the tracking down of the perpetrator. The police have explained, as discussed in the confidential annex, how the information in the report has been, and is being, used in the investigation.

17. The Commissioner accepts there is a real risk of prejudicing the investigation should this information be disclosed as it would give the

perpetrator an insight into the investigation and the methods employed by the police.

18. The Trust has made a further argument that disclosure of the NCC report would prejudice the prevention of crime in the future by exposing other organisation and the Trust to hacking attacks in the future. It argues that the NCC report describes and analyses the route of hacking used against the Trust and does so in such detail it could be used a 'how to' guide for attacking other systems in other organisations. Further detail on this is provided in the confidential annex.

19. The Trust, based on the advice from the police and NHS Digital (the national body responsible for cyber security guidance to the NHS) considers that disclosure of the NCC report would increase its vulnerability to cyber-attacks. The technical detail in the report could be exploited to disrupt the Trust's IT in the future and could make it more difficult to prevent future attacks.

20. The Commissioner accepts there is a genuine risk of the information being able to be used by other hackers to exploit vulnerabilities at other organisations, the level of detail in the report including diagrams would be of some interest or use to motivated individuals. Exposing other organisations to increased risk would then have an impact on the police's ability to prevent cyber-crime as information would be placed in the public domain which could potentially make attacks easier to carry out.

21. The Commissioner therefore finds that sections 31(1)(a) and (b) are engaged as it would prejudice the police's functions of detecting and preventing crime and prosecuting and apprehending offenders, specifically in relation to the cyber-attack on the Trust. Section 31 is a qualified exemption and the Commissioner must therefore consider the public interest test before reaching a conclusion.

Public interest arguments in favour of disclosure

22. The Trust has recognised the public interest in the disclosure of information that increases transparency and demonstrates accountability within public authorities.

23. The Trust also accepts that disclosing the report would help to inform technically accurate debate around cyber-security and the facts of the incident. The Trust states there has been some inaccurate reporting of the attack and has attempted to mitigate this by issuing its own public statements but acknowledges disclosing the report would go further than this by providing a factually and technically accurate account of the attack. That being said, the Trust argues the public interest is more in

the debate around NHS IT security and the NCC report would not particularly add to this as it is highly specific to the Trust.

24. The Trust acknowledges that the NCC report relates to a serious incident affecting the provision of services by the Trust and there is a public interest in assuring the public that IT security issues are being taken seriously. Again the Trust argues this public interest can be met in other ways than through disclosure of the NCC report, for example the Trust is subject to regulatory and system controls and is accountable to NHS commissioners who have been fully briefed on the incident.

Public interest arguments in favour of maintaining the exemption

25. The Trust points to the inherent public interest in avoiding the prejudice covered by the exemption itself. Specifically, the strong public interest in the proper conduct of investigations, particularly where it may lead to criminal proceedings.

26. The Trust has also referenced a decision of the Upper Tribunal[1] which found that one of the factors that can be taken into account in weighing the public interest test is avoiding the consequences that accompany or follow criminal acts. The Trust also points to the Commissioner's own guidance on this[2] in which she finds that there is a *"clear public interest in protecting society from the impact of crime. The greater the potential for a disclosure to result in crime, the greater the public interest in maintaining the exemption. The victims of a crime can be both organisations and individuals."* The Trust therefore argues there could be significant social consequences from a successful attack and this would not be in the public interest.

Balance of the public interest arguments

27. The Commissioner recognises the public interest in the disclosure of information which encourages transparency and accountability and she accepts there will be a public interest in information which shows how the NHS are dealing with cyber-attacks and that they have learned

---

[1] http://informationrights.decisions.tribunals.gov.uk/DBFiles/Appeal/i560/UT%20Decision_[2012]UKUT190(AAC)_2012-06-06.pdf

[2] https://ico.org.uk/media/for-organisations/documents/1207/law-enforcement-foi-section-31.pdf

lessons to ensure they have sufficiently robust IT systems going forwards.

28. That being said, the Commissioner considers the Trust makes a valid point that the NCC report is a technical document analysing the attack and does not necessarily contain information which would meet the public interest in understanding how effective NHS IT services are. Therefore, whilst the Commissioner accepts there would still be some public interest in the information in the report she does not consider this to be an argument that carries much weight.

29. In contrast, the Commissioner recognises the importance of the police being able to carry out its functions effectively. The Trust has demonstrated that disclosure would prejudice the police's functions of preventing and detecting crime and apprehending and prosecuting offenders and the Commissioner accepts it is in the public interest for the police to be able to use the information in the NCC report to continue its investigation effectively. The public interest argument for withholding the information in the NCC report is therefore strong.

30. As wel as this the Commissioner has factored in the impact of disclosure on not just the ability of the police to apprehend and prosecute an individual responsible for this cyber-attack; but also the impact on the police's ability to prevent and detect future crimes and the possibility that the information in the report might provide a 'how to' guide for hackers to carry out other attacks. It is not in the public interest to hinder the police in their attempts to reduce cyber-crime and ensure that NHS services can remain uninterrupted.

31. Taking all of this into account the Commissioner considers there are strong arguments for maintaining the exemption to allow the police to continue their ongoing investigation and attempt to apprehend the perpetrator of the cyber-attack as well as ensuring the highly detailed technical information stays out of the public domain where it can be utilised by any individual motivated to carry out a similar attack.

32. Therefore the Commissioner finds that the public interest in favour of disclosure is outweighed by the public interest in maintaining the exemption.

33. As she has found that section 31 has been correctly applied the Commissioner has not gone on to consider section 36(2)(c).

Right of appeal

34. 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@hmcts.gsi.gov.uk
    Website: www.justice.gov.uk/tribunals/general-regulatory-chamber

35. 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.

36. 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 ……

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