

Freedom of Information Act 2000 (FOIA)

Decision notice

Date: 12 June 2019

Public Authority: Parliamentary and Health Service Ombudsman
Address: Millbank Tower
Millbank
London
SW1P 4QP

Decision (including any steps ordered)

1. The complainant has requested copies of the Parliamentary and Health Service Ombudsman's (PHSO)'s Security Guidance and its Security Operating Procedures. The PHSO provided a copy of the Security Operating Procedure and a limited amount of information from the Security Guidance. It withheld the rest of the information from the guidance under section 31 – law enforcement.
2. The Commissioner's decision is that section 31 does not apply to all the information which the PHSO is continuing to withhold. By failing to communicate the information not protected by the exemption, the PHSO has breached section 1 of the FOIA.
3. The Commissioner requires the public authority to take the following steps to ensure compliance with the legislation.
 - To disclose the information which does not engage the exemption provided by section 31. This information is identified in a confidential annex which has been provided solely to the PHSO.
4. The public authority must take these steps within 35 calendar days of the date of this decision notice. Failure to comply may result in the Commissioner making written certification of this fact to the High Court pursuant to section 54 of the Act and may be dealt with as a contempt of court.

Request and response

5. On 23 August 2018 the complainant wrote to the PHSO commenting on the information he had received in response to an earlier request. At the end of that letter, under the heading 'Additional Comments' he made a fresh information request in the following terms:

"Could you please raise a Freedom of Information request for the following documents?

Security Guidance for further details on handling arrangements for electronic information.

Security Operating Procedures (SyOPs)."

6. On 1 October 2018 the PHSO responded. It refused to provide the requested information. The PHSO cited the exemption provided by section 31(1)(a) – law enforcement – prejudice to the prevention or detection of crime, as its basis for doing so.
7. The complainant requested an internal review on the same day, i.e. 1 October 2018. The PHSO sent him the outcome of its internal review on 31 October 2018. It revised its position and disclosed a copy of the Security Operating Procedures (SyOPs), but continued to withhold the Security Guidance under section 31.
8. During the course of the Commissioner's investigation the PHSO disclosed a limited amount of information from the Security Guidance. This was provided to him in May 2019.

Scope of the case

9. The complainant contacted the Commissioner on 8 November 2019 to complain about the way his request for information had been handled.
10. The Commissioner considers the matters to be decided is whether the exemption provided by section 31(1)(a) is engaged in respect of the information which the PHSO is continuing to withhold from the Security Guidance and, if so, whether the public interest favours maintaining that exemption.

Reasons for decision

Section 31(1)(a) – law enforcement

11. The Commissioner recognises that the complainant said, when seeking an internal review, that he had no intention of passing the withheld information on to anyone else. However a disclosure made under the FOIA is considered to be a disclosure to the world at large. Therefore when considering whether the exemption is engaged, the correct test to apply considers what the consequences would be if the withheld information was placed in the public domain, rather than what use the complainant may make of it.
12. The Commissioner also notes that when a limited amount of information from the Security Guidance was provided to the complainant during the course of the investigation, he queried whether he had in fact been provided with information from the correct document. This was because the title page of the document stated that the guidance had been produced in November 2015, whereas the footer suggested the information was from a version that had been revised in December 2014. The PHSO has explained that this was simply a case of human error; when the document was updated in November 2015, the PHSO neglected to amend the footer. The Commissioner accepts this as a plausible explanation. She is satisfied that the PHSO identified the correct document when providing information to the complainant and when providing the Commissioner with a full unredacted version of the guidance for the purposes of her investigation.
13. Section 31(1) of the FOIA states that information, which is not covered by virtue of section 30, is exempt if its disclosure would, or would be likely to, prejudice –
 - a. the prevention or detection of crime.
14. As stated within the exemption itself, this provision is not available to information which is already covered by section 30. In broad terms section 30 exempts information which has been held for the purposes of conducting a criminal investigation which the public authority itself is responsible for conducting, or which relates to obtaining information from confidential sources for such purposes. The Commissioner is satisfied that the withheld information is not protected by section 30. Therefore section 31 is available to the PHSO.
15. Section 31 is a prejudice based exemption which can be applied on the basis that the alleged prejudice either 'would' occur, or that it would only be 'likely' to occur. In this case the Commissioner understands the PHSO's position to be that the prejudice to prevention or detection of crime is likely to occur. The term 'likely' is taken to mean that there is a real and significant risk of the alleged harm occurring. Applying this lower threshold may make it easier to engage the exemption, but the

application of section 31 is subject to a public interest test and when considering that test, less weight is given the public interest in preventing a prejudice that is only likely to occur.

16. When considering a prejudice based exemption the first issue is whether the prejudice envisaged by the public authority is one which the exemption is designed to guard against. In this case the PHSO is concerned, in broad terms, that disclosing the withheld information would aid what it describes as 'malicious actors' to commit various forms of fraud by masquerading as PHSO officials in order to extract information from either the PHSO itself or from third parties such as members of the public. Clearly this is the sort of activity that the exemption is designed to protect against.
17. The PHSO has explained that it has been, and continues to be, targeted by malicious actors and cyber trolls who actively combine information released under various information requests with that which is already in the public domain. It has had cause to report phishing attacks and other forms of fraud to the police in the last 12 months. The forms of attack have included people pretending to be senior managers (known as spear phishing), staff from its accounts department, clinicians and sending out correspondence which purports to be from the PHSO and emails designed to simulate its security technologies. The Commissioner therefore accepts that are malicious actors who present a real risk to the PHSO and the wider public.
18. However before accepting the exemption is engaged the Commissioner needs to consider whether there would be a causal link between the disclosure of the actual information that is being withheld and the prejudice claimed, i.e. would disclosing this information actually provide these malicious actors with intelligence that would make it easier for them to access information that would make it easier for them to perpetrate fraud.
19. The PHSO has identified a wide range of information that is contained in the Security Guidance which it believes could aid an attacker. It would not be appropriate for the Commissioner to list all the types of information or explain exactly how it could be used by fraudsters. However some simple examples include information on the roles and responsibilities of staff involved in managing security risks, the disclosure of which could aid 'spear phishing', details of security checks, password protocols, how documents are transferred within the PHSO and between itself and other public authorities.
20. The arguments presented by the PHSO appear logical, however the Commissioner has gone through the withheld information. Some of the guidance it contains covers very basic measures. It is difficult to accept that disclosing such information would actually add to a fraudster's

knowledge of the organisation in any meaningful way. The Commissioner is not satisfied that the exemption is engaged in respect of such information.

21. The Commissioner has also compared the withheld information with that which is in the public domain by virtue of being contained in documents that have already been published by the PHSO. Where the withheld information is the same as that already public domain, or is so similar that it conveys no new intelligence of use to fraudsters, the Commissioner finds its disclosure would not prejudice the prevention of crime. Such information does not engage the exemption. In reaching this conclusion the Commissioner has taken account of whether disclosure of the withheld information would assist fraudsters by, in effect, bringing together information that they would otherwise need to search through a number of documents to locate. Having considered this point the Commissioner is satisfied that only a limited number of documents would need to be searched to bring the information together and so it can be considered to be already easily accessible.
22. However the remaining information that has been withheld is of a different character. It provides details of security measures adopted by the PHSO as well as its procedures for handling, storing and transferring information. It includes details relating to the handling of incoming post. The disclosure of this information would present some very obvious security risks. The withheld information includes details of naming and labelling conventions and the use of protective markings. It also explains in some detail the roles and responsibilities which specific staff have for security issues; this would allow fraudsters to present themselves more convincingly when 'phishing'. Other information discusses the security issues relating to particular circumstances and in doing so identifies potential vulnerabilities. The disclosure of such information would increase the risks associated with those situations.

The Commissioner is therefore satisfied that the disclosure of this information would increase the security risk to the PHSO's staff, its physical assets and the information it holds. This in turn could undermine the security of third parties about whom the information relates. The Commissioner finds that the exemption is engaged in respect of this information.

Public interest test

23. Section 31 is subject to the public interest test as set out in section 2 of the FOIA. This means that even though the exemption is engaged in respect of the remaining information, it must still be released unless the public interest in maintaining the exemption is greater than the public interest in disclosing it. When conducting this test the Commissioner has had regard for the fact the PHSO has engaged the exemption on the

lower threshold, i.e. that it considers the prejudice to the prevention of crime is only likely to happen. This decreases the weight the Commissioner will attribute to the harm that releasing the information would have.

24. There will always be a public interest in a public authority such as the PHSO being transparent and open. This increases accountability. It allows the public to better understand how the organisation works, whether it is providing value for the public money it spends. It also allows informed debate about how that body is performing.
25. The PHSO has recognised that, over and above these general public interest arguments, there is a public interest in the disclosure of information that would provide assurance to the public on the security of its systems and therefore how secure the information it handles is. However the PHSO goes on to argue that the request seeks the details of its security measures rather than information on how effective those security measures are in protecting its information.
26. When seeking an internal review, the complainant commented that disclosure would help him understand how the PHSO's processes work, or whether in fact those processes do not work.
27. The Commissioner considers that providing the information would allow one to take an informed view of whether the PHSO has put in place appropriate measures to protect the information it holds together with the security of its physical assets and its staff. Even though the requested information does not capture details of any security breaches, or how many phishing attacks were detected and prevented, the information would still help the public form an opinion on whether the procedures that were in place were likely to be effective.
28. In performing its statutory functions the PHSO processes a lot of information, including the personal data of members of the public who have raised concerns with it. There is therefore a very real value in the public having confidence that any information they provide to the PHSO will be handled securely and that by providing information to the PHSO, they are not making themselves vulnerable to fraud.
29. However in this case the very act of disclosing the requested information would place the information held by the PHSO at greater risk from malicious actors. This would directly undermine any value in its disclosure, i.e. as a result of disclosing the information the public would have much less confidence that any information which they, or the public bodies covered by the PHSO, provided, could be held securely. This would seriously compromise the ability of the PHSO to carry out its legislative duties. This is a very weighty public interest argument in favour of maintaining the exemption.

30. In addition to that argument is the public interest in preventing the PHSO, or other parties, including members of the public and PHSO's contractors, actually becoming targets and victims of fraud through the use of information obtained by phishing attacks.
31. The Commissioner is satisfied that the public interest in maintaining the exemption, and preventing any erosion to the security with which the PHSO holds information, is greater than the public interest in disclosure. The PHSO is entitled to withhold the remaining information under section 31(1)(a).

Right of appeal

32. 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

33. 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.
34. 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

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