

Freedom of Information Act 2000 (FOIA)

Decision notice

Date: 26 January 2022

Public Authority: Yorkshire Ambulance Service NHS Trust

Address: Ambulance Headquarters
Springhill
Brindley Way
Wakefield 41 Business Park
Wakefield
WF2 0XQ

Decision (including any steps ordered)

1. The complainant has requested information relating to an incident that Yorkshire Ambulance Service NHS Trust ('the Trust') supposedly attended.
 2. The Trust would neither confirm nor deny that it held the requested information, citing section 40(5B)(a)(i) (personal information) of the FOIA.
 3. The Commissioner's decision is that section 40(5B)(a)(i) is not engaged.
 4. The Commissioner requires the Trust to take the following steps:
 - Issue a fresh response, which must confirm or deny whether the information is held, and either disclose the requested information or issue a valid refusal notice compliant with section 17 of the FOIA.
-

Request and response

5. On 8 July 2021 the complainant wrote to the Trust and requested information in the following terms:
6. “[Redacted]
 1. I would like to see the incident log please.
 2. The times and details of the YAS resources involved (type of vehicle and where based, staff numbers and rank/position).
 3. Additionally, please contact any contact with other emergency services, the time of that contact, and their responses to your contact with them.”
7. The Trust responded on 14 July 2021, refusing to confirm or deny that it held the requested information.
8. Following an internal review the Trust wrote to the complainant on 19 July 2021. It upheld its original position.

Scope of the case

9. The complainant contacted the Commissioner on 20 July 2021 to complain about the way that their request for information had been handled.
10. The complainant was specifically concerned that ‘None of the detail sought is in any way “personal”’.
11. The Commissioner considers the scope of his investigation to be to determine if the Trust is entitled to rely upon section 40(5B)(a)(i) as a basis for refusing to neither confirm or deny whether it held the requested information.

Reasons for decision

Neither confirm nor deny (NCND)

12. Section 1(1)(a) of the FOIA requires a public authority to inform a requester whether it holds the information specified in a request.
13. However, there may be occasions whereby complying with section 1(1)(a) would itself disclose information which would be covered by the relevant exemption. In circumstances such as this the public authority

may respond by neither confirming nor denying whether it holds the requested information.

14. The decision to use a NCND response will not be affected by whether a public authority does or does not hold the requested information. The key issue for NCND in most cases will be theoretical considerations about the consequences of confirming or denying whether the information is held.
15. The Trust could easily deny holding the requested information if this incident had not been attended. However, the Commissioner accepts that a public authority may need to issue a NCND response consistently, over a series of separate requests, regardless of whether it holds the requested information. This is to prevent refusing to confirm or deny being taken by requesters as an indication of whether or not information is in fact held.
16. The Commissioner considers the fact that the complainant has provided a very specific description of the event with which they are concerned is relevant to this case. The complainant may be confident that the Trust attended such an incident. However, confirmation under the FOIA is confirmation to the world at large. The Trust believes that, in confirming or denying information is held in relation to the request, would, in itself, disclose personal data.
17. To reiterate, the Commissioner does not need to consider whether the Trust holds the information or the disclosure of any requested information that may be held. The Commissioner need only consider whether the Trust is entitled to NCND whether it holds any information in relation to the request.

Section 40 - Personal information

18. Section 40(2) of the FOIA states:

“Any information to which a request for information relates is also exempt information if-

- (a) It constitutes personal data which does not fall within subsection (1), and
- (b) The first, second or third condition below is satisfied.”

Subsection (1) refers to exempt information that constitutes personal data of which the applicant is the data subject.

19. In this instance the relevant condition is contained in section 40(3A)(a) which states:

"The first condition is that the disclosure of the information to a member if the public otherwise than under this Act-

Would contravene any of the data protection principles."

20. The Commissioner considers that the lawful basis most applicable is basis 6(1)(f) which states:

"processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data."

21. Section 40(5B)(a) states:

"The duty to confirm or deny does not arise in relation to other information if or to the extent that any of the following applies—

(a)giving a member of the public the confirmation or denial that would have to be given to comply with section 1(1)(a)—

(i)would (apart from this Act) contravene any of the data protection principles".

22. For the Trust to be entitled to rely on section 40(5B)(a)(i) of FOIA to refuse to confirm or deny whether it holds information falling within the scope of the request, the following two criteria must be met:

- Confirming or denying whether the requested information is held would constitute the disclosure of a third party's personal data; and
- Providing this confirmation or denial would contravene one of the data protection principles.

Is the exemption engaged?

22. The first step for the Commissioner is to determine whether, if providing confirmation or denial that information is held in relation to the request would disclose personal data as defined by the Data Protection Act 2018 ('DPA18'). If this is not the case, then section 40(5B)(a)(i) cannot be used as a basis for refusing to confirm or deny whether the information is held.

23. Part 1, Section 3(2) of the DPA18 defines personal data as:

"any information relating to an identified or identifiable living individual."

24. The two main elements of personal data are that the information must relate to a living person and that the person must be identifiable from that information.

25. Information will relate to a person if it is about them, linked to them, has biographical significance for them, is used to inform decisions affecting them or has them as its main focus.
26. An identifiable living individual is one who can be identified, either directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.
27. To assist the Commissioner with his investigation, the Trust explained what type of information would be held on an incident log. It would include health data relating to the patient (or patients), and 'descriptions of vehicles (should the matter relate to a road traffic collision), accurate descriptions of injuries, telephone contact numbers, the name of the caller and patient (should the two be separate) and any other pertinent information, demographic information (name, date of birth, sex/gender etc.) along with medical history, presenting complaint, social circumstances, care planning, treatment, and any safeguarding matters.'
28. The Trust has explained 'to confirm that it held this data would be to confirm that there was indeed a patient, requiring urgent medical assistance for a health need, at that date and time at that location.'
29. The Commissioner agrees. If the Trust confirms that it holds information in response to the request, it is confirming the existence of a patient who was attended to at the date and time in question. To deny information is held would be to confirm that no such incident was attended.
30. However, returning to section 1(1)(a), a public authority has a duty to confirm or deny that information is held in response to a request unless doing so would disclose information which would be covered by the relevant exemption.
31. Returning to the request itself, there is no individual named within it. Therefore the Commissioner did not agree that either confirming or denying information is held would disclose the identity of any patient, or any further information relating to an identifiable individual. To reiterate, the Trust can only engage section 40(5B)(a)(i) if complying with section 1(1)(a) would, in itself, disclose personal data.
32. Therefore, the Commissioner returned to the Trust and asked it to reconsider its position. The Commissioner explained that, for the Trust to be able to rely upon section 40(5B)(a)(i) to neither confirm nor deny that it holds information in relation to this request, it must explain **how** such confirmation or denial would identify the patient or any further information relating to an identifiable individual. The Commissioner

asked the Trust to consider how an individual, with no prior knowledge of the incident in question, could derive personal data from such confirmation or denial.

33. The Trust returned and noted that the request contains the date, location, and time of an alleged incident. The Trust explained that it had real concerns that the complainant's prior knowledge of any such incident might be combined with any confirmation or denial that the Trust would provide.
34. Again, the Commissioner agrees. His guidance 'Anonymisation: managing data protection risk code of practice'¹ states 'The risk of re-identification posed by making anonymised data available to those with particular personal knowledge cannot be ruled out, particularly where someone might learn something 'sensitive' about another individual – if only by having an existing suspicion confirmed.'
35. The Trust has explained that it used the aforementioned guidance to inform its handling of the request, bearing in mind that any information contained within an incident log is likely to contain special category data. The Trust noted that, if a patient is attended to by an ambulance, they are likely to be distressed during the incident and the degree of embarrassment or anxiety that re-identification could cause could be very high.
36. The Commissioner's guidance states, 'In borderline cases where the consequences of re-identification could be significant eg because they would leave an individual open to damage, distress or financial loss, organisations should: adopt a more rigorous form of risk analysis and anonymisation.'
37. The Commissioner is in complete agreement with the Trust. Should the identity of any patient attended by the Trust be disclosed in response to an FOIA request, this may cause distress and would need to be overridden by the legitimate interests of the request in order to be lawful.

¹ [Anonymisation: managing data protection risk code of practice \(ico.org.uk\)](https://ico.org.uk)

The Commissioner's view

38. The Commissioner does not consider section 40(5B)(a)(i) is engaged in this instance.
39. If the Trust confirms that it holds information in relation to the request, it confirms the existence of a patient and an incident. If it denies it, it denies the existence of a patient and an incident.
40. The Trust has clearly adopted a rigorous form of risk analysis to determine whether such information could be linked to an individual. However, the Trust has been unable to explain to the Commissioner **how** such confirmation or denial would identify a specific patient or reveal further information about an identifiable individual. In the Commissioner's opinion, the Trust can confirm or deny that it holds information in relation to the request.
41. The requestor clearly believes an incident took place at the date and time specified in the request. If the Trust confirms the existence of this incident this does not, in itself, give the requestor any new information, it is just confirming what the requestor already knows. It does not disclose the identity of the patient or any personal data relating to an identifiable individual.
42. The Trust has stated that the request does not appear to have stemmed from any information already in the public domain. The Commissioner agrees that there does not appear to be any information within the public domain that could allow a member of the public to piece together information, with the confirmation or denial the Trust would provide, to determine the identity of any patient. Whilst the requestor suspects that an incident has occurred, the Trust has failed to explain how confirming or denying it holds information in relation to the request would, in itself, disclose information that section 40 is designed to protect.

Other matters

43. To reiterate, a public authority has two obligations according to section 1(1)(a): to inform a requester whether it holds the information specified in a request and to disclose it unless an exemption applies.
44. It is likely that, given the circumstances of the request, any information that the Trust may hold may engage section 40(2) and represent special category data. The appropriateness of disclosure would be a separate matter for the Commissioner to consider.

Right of appeal

45. 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: 0203 936 8963

Fax: 0870 739 5836

Email: grc@justice.gov.uk

Website: www.justice.gov.uk/tribunals/general-regulatory-chamber

46. 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.
47. 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

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