Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
T. 0303 123 1113 F. 01625 524510

21 June 2023

IC-234672-Z9M2

Request

You asked us:

"1. I refer to the article in the Guardian/Observer newspaper dated 14th May 2023[…].

2. I note the comment attributed to your spokesman in the final paragraph. I appreciate that the comment may have been edited beyond comprehension, or taken out of context, but I cannot see a concurrent related news release by the ICO. Has the ICO undertaken a substantive investigation of this case, or was this a provisional remark by a press officer? If there was a more expansive statement, I would be grateful if you would provide a copy. What was the comment intended to convey?

3. As described, this case, provides prima facie evidence of various breaches of various data protection and privacy laws by an individual, but also institutionally. I struggle with the apparent conclusion that the ICO has no reactive regulatory role. I would be grateful if you would provide clarification. If an investigation has been undertaken, the analysis concluding that no action should be taken by the ICO in this case, would be helpful.

4. As a minimum, what steps have been taken by the ICO to inform the affected data subject of her rights under the information legislation so that she can be empowered to raise an informed complaint to your office?

5. Particularly, has the ICO investigated if the data subject was provided with the fair processing information prior to the consultation with her GP? If so, did that fair processing information sufficiently, accurately and clearly inform the patient of her right to prevent her sensitive information, that was recorded in the GP surgery, being rendered accessible (or transferred) to other data controllers more

widely across the National Health Service? This would include fulfilment of the common law obligation of consent. Has the ICO reviewed the enhanced standard required for common law consent, in the medical setting, since the judgement in Montgomery v Lanarkshire Health Board? Given the potentially life changing detriment attached to information release with inadequate consent, the rationale set out in that judgement applies in respect of release of patient information, even to the wider NHS.

6. Did the fair processing information make it clear that it is wholly reasonable for patients to conclude that they do not want their medical information, as a whole or in part, to be rendered accessible across different NHS organisations? Or was the fair processing information weighted by dubious reassurances and none-specific, misleading implications of detriment to care if such consent is withheld? […]

10. In a case of this nature, does the ICO or the Police service have primacy in respect of 1. the conduct of an investigation and 2. the decision to prosecute?"

We have handled your request under the Freedom of Information Act 2000 (the FOIA).

The article referred to is entitled *"Warnings over NHS data privacy after 'stalker' doctor shares woman's records,"* and was published in *The Guardian* on 14 May 2023. We have abridged some content of your above correspondence with the ICO where it does not directly constitute an information request.

Our response

We can confirm that we hold some of the information you have requested. We address your queries separately below.

2. I note the comment attributed to your spokesman in the final paragraph. I appreciate that the comment may have been edited beyond comprehension, or taken out of context, but I cannot see a concurrent related news release by the ICO. Has the ICO undertaken a substantive investigation of this case, or was this a provisional remark by a press officer? If there was a more expansive statement, I would be grateful if you would provide a copy. What was the comment intended to convey?

The comment in question is a quote from the article, which states, *"The information commissioner said it had no power to help the woman and that it was CUH, and not her, that the data breach had affected."*

We can confirm that the comment in question is not drawn from a press statement from the ICO to *The Guardian*.

However, the ICO did provide press statements to *The Guardian* in relation to the incident upon request.

On 12 May, the ICO's press office provided the following statement to *The Guardian*:

> *"People's medical data is highly sensitive information, not only do people expect it to be handled carefully and securely, organisations also have a responsibility under the law.*
>
> *"When a data incident occurs, we would expect an organisation to consider whether it is appropriate to contact those affected, and to consider whether there are steps that can be taken to protect them from any potential adverse effects.*
>
> *"Cambridge University Hospitals NHS Foundation Trust made us aware of an incident. After carefully reviewing the information provided, we gave data protection advice and recommendations and closed the case with no further action".*

On 16 May, following the article's publication, the ICO's press office provided a further statement to *The Guardian* from the Information Commissioner, John Edwards:

> *"Every one of us expects that our medical data will be handled carefully and securely, and data protection law exists to ensure that happens. The details reported in the Guardian on Monday suggest an attitude to people's health records that is not acceptable.*
>
> *"The ICO has already made clear recommendations to Cambridge University Hospitals NHS Foundation Trust, particularly around how patient records can be viewed, to prevent something like this happening again. But I've asked my team to reopen their investigation into what happened in this case, to ensure both the person who raised this case with us, and patients more widely, can have confidence in how their information is looked after."*

While we are unable to comment on this specific incident, I can advise that an

incident in which an individual has obtained or disclosed personal data held by a data controller without the data controller's consent is an offence under section 170 of the Data Protection Act 2018 (DPA). A section 170 offence is one in which the data controller is the victim, and in its enforcement capacity, the ICO must consider section 170 investigations from this perspective.

Affected data subjects can of course raise their concerns with the ICO regarding an organisation's data processing as a data protection complaint, and our investigations may be informed by complaints raised by members of the public. However, it is important to note that the ICO are not able to pursue legal claims on an individual's behalf.

3. As described, this case, provides prima facie evidence of various breaches of various data protection and privacy laws by an individual, but also institutionally. I struggle with the apparent conclusion that the ICO has no reactive regulatory role. I would be grateful if you would provide clarification. If an investigation has been undertaken, the analysis concluding that no action should be taken by the ICO in this case, would be helpful.

4. As a minimum, what steps have been taken by the ICO to inform the affected data subject of her rights under the information legislation so that she can be empowered to raise an informed complaint to your office?

5. Particularly, has the ICO investigated if the data subject was provided with the fair processing information prior to the consultation with her GP? If so, did that fair processing information sufficiently, accurately and clearly inform the patient of her right to prevent her sensitive information, that was recorded in the GP surgery, being rendered accessible (or transferred) to other data controllers more widely across the National Health Service? […]

6. Did the fair processing information make it clear that it is wholly reasonable for patients to conclude that they do not want their medical information, as a whole or in part, to be rendered accessible across different NHS organisations? Or was the fair processing information weighted by dubious reassurances and none-specific, misleading implications of detriment to care if such consent is withheld?

We are unable to comment on the details of an individual's complaint or correspondence with the ICO where this constitutes the personal data of the complainant. Information regarding this has therefore been withheld under section 40(2) of the FOIA.

Disclosure of this data would break the first principle of data protection - that personal data is processed lawfully, fairly and in a transparent manner.

There is no strong legitimate interest that would override the prejudice that disclosure would cause to the rights and freedoms of the individuals concerned. So we are withholding the information under section 40(2) of the FOIA.

We are, however, able to confirm that CUH self-reported the personal data breach and that an ICO investigation into the incident is currently ongoing. Further details of the investigation regarding this matter have been withheld under section 30 of FOIA.

Section 30(1) states that:

"Information held by a public authority is exempt information if it has at any time been held by the authority for the purposes of-

(a) any investigation which the public authority has a duty to conduct with a view to it being ascertained-
(i) whether a person should be charged with an offence, or
(ii) whether a person charged with an offence is guilty of it,
(b) any investigation which is conducted by the authority and in the circumstances may lead to a decision by the authority to institute criminal proceedings which the authority has power to conduct, or
(c) any criminal proceedings which the authority has power to conduct."

Section 30 is not an absolute exemption. This means we need to carry out a public interest test.

Factors in favour of disclosure:

- There is a general public interest in transparency regarding the ICO's functions.
- There is a strong public interest in data protection as it applies to public healthcare and the processing of sensitive medical data.

Factors against:

- Disclosure under FOIA is disclosure to the wider world, and if the ICO were to reveal the details of an investigation prematurely, that might alert any relevant parties and enable them to take steps to frustrate the ICO's investigations.

- Disclosure would also risk highlighting intelligence and evidence that may be pertinent to the success of future investigations.
- Further, if the ICO were to reveal the details of an investigation prematurely, this could prejudice the ICO's ability to conduct future investigations, as this may affect the willingness of relevant parties in the future to co-operate with the regulator.
- The public interest is served by our commitment to publish noteworthy criminal investigations in due course as published in our "Communicating our Regulatory and Enforcement Activity Policy"

Having considered these factors, we are satisfied that we can rely on section 30 to withhold the information you have requested.

6. […] Has the ICO reviewed the enhanced standard required for common law consent, in the medical setting, since the judgement in Montgomery v Lanarkshire Health Board? Given the potentially life changing detriment attached to information release with inadequate consent, the rationale set out in that judgement applies in respect of release of patient information, even to the wider NHS.

We have consulted with our Legal Services (Regulatory Enforcement Directorate) and can confirm that no information was held at the point of consultation.

It is important to note that 'consent' in the context of data protection is distinct from other forms of consent, such as medical or common law consent. Concerns primarily relating to medical or common law consent lie beyond the remit of the data protection legislation.

You can find more information on consent in a data protection context on our website, including our detailed guidance on consent and explicit consent for organisations.

In a case of this nature, does the ICO or the Police service have primacy in respect of 1. the conduct of an investigation and 2. the decision to prosecute?

Both the ICO and the police can prosecute a DPA offence. Which organisation takes "primacy" is based on the individual circumstances of a case.

This concludes our response to your information request.

Next steps

You can ask us to review our response. Please let us know in writing if you want us to carry out a review. Please do so within 40 working days.

You can read a copy of our full review procedure here.

If we perform a review but you are still dissatisfied, you can complain to the ICO as regulator of the FOIA. This complaint will be handled just like a complaint made to the ICO about any other public authority.

You can raise a complaint through our website.

Your information

Our Privacy notice explains what we do with the personal data you provide to us, and set out your rights. Our retention schedule can be found here.

Yours sincerely

Information Access Team
Strategic Planning and Transformation
Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
ico.org.uk twitter.com/iconews
Please consider the environment before printing this email