Information Commissioner's Office

Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524 510 www.ico.org.uk

The Information Commissioner's response to request for feedback on the National Data Guardian's draft guidance for Caldicott Guardians

Following the National Data Guardian's (NDG) consultation on the Caldicott Guardians and principles, she plans to issue guidance under her statutory powers. This guidance, when implemented, will mean that more organisations across health and adult social care should have a Caldicott Guardian than are currently advised to have one.

In preparation for this, the Office of the National Data Guardian asked stakeholders to provide feedback on the first draft of the guidance – **by 29 January 2021.**

Below is the ICO's feedback on the first draft of the guidance.

- The geographical scope of the new Caldicott principles should be flagged early in the document for the benefit of readers in the devolved administrations.

- There is potential for confusion in the use of the term 'confidential'. There is a risk that readers may be unaware of the difference between confidentiality under the Common Law Duty of Confidence and the responsibilities under the GDPR to keep personal data secure and share it only with an appropriate lawful basis, and in the case of special category data an additional Article 9 processing condition.

- It would be beneficial for Caldicott Guardians to receive training in the GDPR to understand the important differences between both as they will have responsibilities under both and will need to communicate the right message to their organisation/s.

- The Caldicott Guardian and the Data Protection Officer (DPO) will need to be regularly in touch with one another to unify the message to their organisation/s regarding how personal data is to be handled under both the GDPR are and the Caldicott principles.

- Caldicott Guardians need to be aware of the potential secondary uses of data for research. There is otherwise a risk that legitimate sharing for

research purposes may be hindered due to a lack of awareness of specific exemptions relating to research under data protection legislation.

Feedback on proposal that DPO and CG roles could be carried out by the same person

The ICO's Relationship Management Service and Innovation Hub met with the Office of the National Data Guardian on 26 January 2021. We were asked about a proposal in the guidance that the **roles of the DPO and Caldicott Guardian could be carried out by the same person** (Paragraph 5.3 in the guidance, p10).

As Article 38(6) of the GDPR states in relation to the position of the DPO: *'The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.'*

As an example of assigning other tasks, Article 30 of the GDPR requires that organisations must maintain records of processing operations. There is nothing preventing this task being allocated to the DPO.

However, as our online guidance explains that the DPO cannot hold a position within the organisation that leads them to determine the purposes and the means of the processing of personal data. At the same time, the DPO shouldn't be expected to manage competing interests that could result in data protection taking a secondary role.

Although the GDPR does not define 'conflict of interests', section 3.5 of the Article 29 Guidelines on DPOs explain that:

'The absence of conflict of interests is closely linked to the requirement to act in an independent manner. Although DPOs are allowed to have other functions, they can only be entrusted with other tasks and duties provided that these do not give rise to conflicts of interests. This entails in particular that the DPO cannot hold a position within the organisation that leads him or her to determine the purposes and the means of the processing of personal data. Due to the specific organisational structure in each organisation, this has to be considered on a case-by-case basis'.

The example (also published in our online guidance) below demonstrates how this 'conflict of interests' could arise.

'A company's head of marketing plans an advertising campaign, including which of the company's customers to target, what method of communication and the personal details to use. This person cannot also be the company's DPO, as the decision-making is likely to lead to a conflict of interests between the campaign's aims and the company's data protection obligations'.

Therefore, while we see the roles of the DPO and Caldicott Guardians as complimentary, we do not see them as compatible for one person to hold simultaneously because of the potential for conflict to arise. If one person carried out both roles, it is inevitable that they would need to make trade-offs. Our position is that data protection compliance must take priority, which may be detrimental to the application of or adherence to the NDG principles.

We hope you find the above feedback helpful. If you would like to discuss any of this further, please email the Relationship Management Service on rms@ico.org.uk

About the ICO

The Information Commissioner has responsibility for promoting and enforcing the UK General Data Protection Regulation ('UK GDPR'), the Data Protection Act 2018 ('DPA'), the Freedom of Information Act 2000 ('FOIA'), the Environmental Information Regulations 2004 ('EIR') and the Privacy and Electronic Communications Regulations 2003 ('PECR'). She is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations, solving problems where she can, and taking appropriate action where the law is broken.