Protecting Patients from Unauthorised Access to Health Records

Overview

The numerous recent incidents of unauthorised access to patient records across the UK are deeply concerning. They cause real distress to patients and their families and risk undermining public trust in the confidentiality of health services.

Organisations must have appropriate measures in place to protect personal information, and people acting under their authority must only access patient information where they are authorised to do so.

You can find guidance on securing personal data on our website:

A Guide to Data Security *<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/a-guide-to-data-security/>*

Access Control *<https://ico.org.uk/for-organisations/advice-and-services/audits/data-protection-audit-framework/toolkits/information-and-cyber-security/access-control/>*

Personal Data Breaches - A Guide *<https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/personal-data-breaches-a-guide>*

You may also wish to refer to sectoral advice and guidance on this topic.

Why your views matter

We are asking you to complete this form to provide assurance that you are taking, or have already taken, the necessary steps to protect the personal data of patients and to ensure that it is only accessed by those staff who need to.

Your responses will shape our continued engagement and response to this issue. We will publish the letter to health leaders that accompanies this form.

Please ensure that you respond via the form. We are not able to accept responses by e-mail and these will not be counted. The contact e-mail address on this page should only be used for technical queries.

View the ICO's privacy notice *<https://ico.org.uk/global/privacy-notice/responding-to-our-consultation-requests-and-surveys/>* to see how we will use the data we collect during this exercise.

Your name, role and organisation

Please provide your full name, role title and the name of your organisation.

Please provide your full name.

Enter your name here *(Required)*

Please provide your organisation's full name.

Please enter the full name of your organisation here *(Required)*

Please confirm your role in your organisation.

Please add your full role title *(Required)*

Effective Access Controls

These questions will allow you to confirm the actions that you are taking to ensure that patient records are appropriately protected from unauthorised access.

The ICO expects health organisations to have role-based access controls. You need to have appropriate security measures in place to prevent the personal data you hold being accidentally or deliberately compromised, which includes having appropriate access controls in place to prevent unauthorised access to patient records.

(Required)

Please select only one item

- ◯ I confirm we have reviewed our organisational policies and procedures relating to access controls in the past six months and I am satisfied that they appropriately address this issue.
- ◯ I commit my organisation to reviewing our policies and procedures regarding this issue in the next three months.
- ◯ Neither of the above.

Effective Monitoring

These questions will allow you to confirm the actions that you are taking to ensure that patient records are appropriately protected from unauthorised access.

The ICO expects health organisations to have effective monitoring and regular audit of access to patient records, with staff made aware that access is monitored. Monitoring should be sufficient to identify unauthorised access to patient records. This includes appropriate logging, routine monitoring, investigation of alerts and the ability to identify access by staff who have no apparent authorised reason to view a record.

(Required)

Please select only one item

- ◯ I confirm we have reviewed our organisational policies and procedures relating to monitoring access in the past six months and I am satisfied that they appropriately address this issue.
- ◯ I commit my organisation to reviewing our policies and procedures regarding this issue in the next three months.
- ◯ Neither of the above.

Regular and Effective Training

These questions will allow you to confirm the actions that you are taking to ensure that patient records are appropriately protected from unauthorised access.

The ICO expects health organisations to have regular, practical training on confidentiality, acceptable access and individual responsibilities. This would include clear communication of reporting and escalation routes, supported by a culture in which unauthorised access is challenged. Staff should understand their responsibilities and the consequences of unauthorised access and breaching confidentiality. Training must be relevant to staff roles and clearly reinforce that accessing records without a legitimate work-related reason, including out of curiosity or for personal purposes, is unacceptable and may be unlawful.

(Required)

Please select only one item

- ◯ I confirm we have reviewed our organisational policies and procedures relating to staff training in the past six months and I am satisfied that they appropriately address this issue.
- ◯ I commit my organisation to reviewing our policies and procedures regarding this issue in the next three months.
- ◯ Neither of the above.

Consistent Action When Things Go Wrong

These questions will allow you to confirm the actions that you are taking to ensure that patient records are appropriately protected from unauthorised access.

The ICO expects that concerns are investigated promptly and consistently with clear accountability for decisions and outcomes. Your organisation should have clear arrangements for investigating suspected unauthorised access, preserving relevant evidence and taking proportionate action. The organisational response may include disciplinary action, or referral to the ICO or other regulators. Personal Data Breaches should be reported to the ICO unless they are unlikely to result in a risk to people's rights and freedoms. You should consider the impact on the person affected and if there is a high risk to their rights and freedoms you should inform them directly, without undue delay.

(Required)

Please select only one item

- ◯ I confirm we have reviewed our organisational policies and procedures relating to disciplinary procedures in the past six months and I am satisfied that they appropriately address this issue.
- ◯ I commit my organisation to reviewing our policies and procedures regarding this issue in the next three months.
- ◯ Neither of the above.

Any Other Information

Is there anything else that you would like to tell us about your organisation's approach to preventing, detecting or responding to unauthorised access to patient records? Please avoid providing identifiable personal data in this section.

Please provide any other relevant information here.