Findings from ICO audits of NHS Trusts under the GDPR

December 2020

Contents

Introduction

The Information Commissioner's Office (ICO) is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

From May 2018 to May 2019 the ICO conducted 12 consensual audits of NHS organisations. These organisations were a combination of Foundation, Health Boards and Ambulance Trusts. Our primary focus was to assess the effectiveness of governance and accountability measures in line with the requirements of the GDPR.

Following each audit, we produced a report that detailed areas of good practice and areas for improvement. Where we identified weaknesses, we made recommendations on how to improve. We then analysed our findings across all the audits we've completed since May 2018, which we have summarised for this report.

Headline areas of concern

During the year since the introduction of the GDPR, we identified some common themes within our audits where Trusts were finding it challenging to implement the necessary measures to comply with the new legislation. The ICO is concerned that a failure to recognise, understand and resolve these issues poses an ongoing risk to the lawful processing and security of the personal data of patients and staff.

Common areas for improvement are outlined below. We have included some examples of practices we experienced during audits, a summary of the recommendations we made in these cases and some practical tips to improve compliance.

Documenting personal data processing

What is required?

Most organisations are required to maintain a record of their processing activities (a ROPA), covering areas such as processing purposes, data sharing and retention. If you have over 250 employees, you must have a ROPA.

A ROPA must include:

- the name and contact details of the organisation (of other controllers, representatives and the DPO where applicable);
- the purpose of the processing;
- a description of the categories of individuals and of the personal data;
- the categories of recipients of the personal data;
- details of transfers to third countries including documenting the transfer mechanism safeguards in place;
- retention schedules; and,
- a description of the technical and organisational security measures.

The Data Security & Protection Toolkit (DSP Toolkit) also has a requirement that organisations should maintain a record or register that details each use or sharing of personal data.

What we found

Most of the Trusts did not have a ROPA in place, some had not even started the process.

Example:
Some Trusts were using their information asset register as a form of ROPA, but we did not believe that these provided the required level of detail.

What we recommend

All Trusts should ensure that they complete a ROPA that covers all internal processing activities. This is a requirement of the legislation (Article 30(1)) and it will also help to demonstrate compliance with other aspects of the GDPR.

Practical Tip:
Completing a data flow mapping exercise is an excellent starting point for creating a ROPA as it will help you to identify all current data processing activities. Document all the data that flows into, around and outside your organisation.

Good Practice:
One Trust has developed an Informatics Portal which provides the functionality for information flow mapping and an information asset register. As information owners or administrators enter details of information assets or systems, links are provided to appropriate policies and procedures and risks can be identified. Reminders are sent a month before the retention date of information assets to alert owners or administrators that there are assets which they need to review and possibly destroy. Entries made on the system are reviewed and users are supported by staff from Information Governance.

For more information about ROPAs please visit the documentation section in the Guide to the GDPR.

Data Protection Officers (DPOs)

What is required?

Following the introduction of the GDPR, all NHS organisations were required to appoint a DPO due the nature of the data they process and their function as a public authority. The 'Key roles and the DPO' guidance within the DSP Toolkit explains the responsibilities and characteristics of the DPO role.

Section 70(5) of the DPA 2018 confirms that the DPO must report to the highest management level within the organisation. In the case of NHS Foundation and Ambulance Trusts, the DPO must have clear and established reporting lines to the executive level Board to ensure that there is effective oversight of data protection compliance across the organisation from the 'top down'.

What we found

In most cases we were concerned that DPOs did not have a clear way to raise data protection concerns with the Board. In addition, NHS DPOs required more support from the central NHS functions and needed to have better contact with each other in order to share knowledge, promote best practice and provide consistency across the system.

DPOs are required to be independent of the decision-making about processing personal data within an organisation. Whilst this separation is necessary to provide independent advice internally, it limits the local or internal support available for DPOs to discuss their concerns and develop their advice.

Example:
One Trust had not provided clear operational independence to the DPO role. This particular Trust had given their DPO financial responsibilities alongside their data protection ones. The DPO's job description included responsibilities for income generation, budgetary controls and development of a financial performance framework. It was our view that these additional responsibilities constituted a conflict of interests that had the potential to distract the DPO from handling their data protection obligations.

A DPO does not have to be just work for one organisation. A DPO can be shared between several smaller organisations, so long as there are appropriate resources available to the DPO and clear reporting lines both to and from the DPO to senior management.

Example:
One of the Trusts had proposed that their DPO could act for local GPs as well. Our concerns in this case were whether each GP surgery would have an equal opportunity to ask for advice and raise issues with the DPO and would the DPO have the time and resources to provide guidance and promote high standards.

What we recommend

The DPO should provide compliance advice and promote good data protection standards. It is a position that, if resourced appropriately, can ensure a high level of compliance in a Trust's data protection practices. The DPO should maintain operational independence and have clear reporting lines to senior management.

Practical tip:
DPOs within a local area or region could establish regular forums to share practices, discuss data protection matters and ensure they apply consistent approaches across their organisations.

For more information about the role of a DPO please visit the DPO section of our Guide to the GDPR.

Requests for access to personal data

What is required?

The right of access, commonly referred to as subject access request (SAR), gives individuals the right to obtain a copy of their personal data as well as other supplementary information. It helps individuals to understand how and why organisations are using their data, and check that they are doing it lawfully. The GDPR does not specify how to make a valid request, and so a patient could make a SAR to a Trust verbally or in writing (including by social media). Individuals can also make a request to any part of the Trust and they do not have to be to direct it to a specific person or contact point.

The DSP toolkit requires Trusts to 'provide details of how access to information requests have been complied with during the last 12 months.' This includes verbal requests.

What we found

Most Trusts had not made specific provisions for how to handle verbal requests. We were also concerned about the quality of the guidance being provided to staff so that they could identify a SAR and channel it to the right person or team. There were members of staff who worked in SAR handling teams who would not accept verbal SARs.

Example:
An Access to Records policy stated that 'all requests should be in writing'.

There was also a lack of more detailed training for SAR handling staff, particularly about how to apply redactions or exemptions when handling SAR requests or what to consider when a request is made by or on behalf of a child.

What we recommend

Trusts should make sure that they have suitable processes in place to record and handle verbal requests and to ensure the identity of the requester.

They should also ensure that all staff are aware of their obligations to treat verbal and written requests for personal data in the same way and they know the process to follow.

Practical tip:
Drafting and implementing a Subject Access Request Policy and supporting procedures is a good way to document your approach to recognising and handling all types of access requests. Communicating this information through role-based guidance with worked examples, followed by regular refresher training and awareness campaigns in key public facing departments is also a good way to ensure staff knowledge remains up to date.

Trusts should provide more in-depth data protection training to SAR handling staff.

Privacy information

What is required?

Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR. Trusts must provide patients with information including:

- their lawful basis and purposes for processing a patient's personal data;
- the retention periods for that personal data; and,
- who it will be shared with.

The Trust should provide this privacy information to patients at the time they collect the personal data. If they obtain patients' personal data from other sources, the Trust should provide patients with privacy information within a reasonable period of obtaining the data and no later than one month. The information they provide to patients must be concise, transparent, intelligible, easily accessible and it must use clear and plain language.

The DSP Toolkit requires Trusts to provide evidence of how they made transparency information (eg a privacy notice) available to the public and how they have informed individuals about their rights and how to exercise them.

What we found

We found that privacy information was only generally provided in one form, for example it was made available on the Trust's external website but not in physical form. There had not been any consideration to providing privacy information in a layered approach, eg patients that did not have access to internet facilities could have accessed the information in another format such as paper-based leaflets or forms.

We were also concerned about the accessibility and availability of the privacy information provided on Trust websites, as these web pages were either difficult to find or did not appear in the search results.

Example:
One Trust did have their privacy information in both paper and electronic form, but the leaflet was out of date and referenced the previous legislation.

There was also a lack of evidence that Trusts had considered the different audiences for the information or proactively 'user tested' the effectiveness of their privacy information to ensure it was appropriate, clear and understandable for every reader.

What we recommend

Actively provide up to date and accurate privacy information to individuals. For privacy information provided through a website, ensure that individuals are aware of it and give them an easy way to access it.

Provide physical privacy information (eg leaflets) in public areas such as reception areas.

Example:
Some Trusts printed out a copy of their privacy notice on request.

Practical tips:
There are a number of techniques you can use to provide people with privacy information:

- ✓ A layered approach – short notices containing key privacy information that have additional layers of more detailed information.
- ✓ Dashboards – preference management tools that inform people how you use their data and allow them to manage what happens with it.
- ✓ Just-in-time notices – relevant and focused privacy information delivered at the time you collect individual pieces of information about people.
- ✓ Icons – small, meaningful symbols that indicate the existence of a particular type of data processing.

- ✓ Mobile and smart device functionalities – including pop-ups, voice alerts and mobile device gestures.

Consider the context in which you are collecting personal data. It is good practice to use the same medium you use to collect personal data to deliver privacy information.

Taking a blended approach and using more than one of these techniques is often the most effective way to provide privacy information.

Trusts should think about the intended audience for their privacy information. For example, for children's personal data, Trusts must take particular care to ensure that the information they provide them with is appropriately written, using clear and plain language.

Practical tip:
It is good practice to carry out user testing on any draft privacy information to get feedback on how easy it is to access and understand.

For more information about privacy notices please visit the right to be informed section in the guide to the GDPR.

Training and awareness

What is required?

A comprehensive data protection training programme is very important to ensure that all staff understand their obligations under the GDPR. It is an effective organisational measure to safeguard personal data and will create a culture of privacy across an organisation.

Under Article 24(2), an organisation should implement appropriate data protection policies to provide guidance for staff in their GDPR responsibilities and to demonstrate that processing is performed in accordance with the legislation. These policies and procedures should form the basis for any staff training.

The DSP Toolkit requires Trusts to provide data protection and security training to new members of staff, either face to face or via e-learning. Trusts must also keep records of what training they have provided and regularly review whether the training remains effective.

What we found

The training provided to locum and agency staff and to data processors was another area of concern. There should be senior management level scrutiny of the training provided to all staff and especially those who are not directly employed by a Trust. If this doesn't happen then there is a risk that some staff don't receiving all the training they need to fulfil their role, which could lead to regulatory action or reputational damage.

There is a lack of evidence that staff have received, read and understood changes to key data protection policies and procedures.

Example:
One Trust notified its staff of policy changes via the intranet only. This meant that clinical staff, who may have limited visibility of the intranet throughout the week, could easily have missed these policy changes.

Induction and refresher training was not always mandatory or completed by all staff, despite the requirement within the DSP Toolkit to provide induction training to new employees.

Example:
There were inconsistencies across all the Trusts we audited. For example, at one Trust not all staff had completed their refresher training. At another, the Senior Information Risk Owner (SIRO) had not completed refresher training.

What we recommend

All Trusts should have a training programme that covers the key areas of data protection. The training should include staff not directly employed by the Trust and all locum, bank staff or volunteers. Trusts should monitor whether staff have completed data protection training and then the DPO should review completion rates and report to the Board.

Trusts should communicate any changes to key data protection policies and procedures to all staff and seek assurances that they have read and understood these changes.

Practical tip:
Trusts could look at the way they communicate changes in data protection policies, procedures or rules to ensure that all staff are updated as soon as possible. Using a multi-layered approach through a variety of communication methods will ensure that they inform all staff about changes in a timely manner. These could include an intranet page, all staff emails or newsletters or bulletin boards.

All new staff should receive basic data protection training as part of their induction. Staff in key roles handling personal data should receive appropriate training prior to

gaining access to systems processing personal data. Existing staff should receive refresher training on a periodic basis.

Practical tip:
The way in which training is administered is at each Trust's discretion, although the most common format is using an e-learning provider. E-learning is useful for ensuring that all staff receive a strong background knowledge in data protection. Trusts can track and report on completion, and staff can consolidate learning through tests or quizzes within their training.

Good practice:
One Trust has developed a TV game show simulation and a live cyber-attack visual feed had been used to increase staff awareness and engagement. This is a creative way of raising awareness around data protection.

Data processor contracts

What is required

Due to the nature and amount of work undertaken by NHS Trusts, it can be the case that support and services are outsourced to other organisations. These organisations act as a processor for a Trust (in their capacity as a controller). Under the GDPR there must be a written contract between a controller and a processor. The contract must include specific minimum terms that clearly set out the obligations, responsibilities and liabilities between the controller and processor.

Contracts must include information about the:
- subject matter and duration of the processing;
- nature and purpose of the processing;
- type of personal data and categories of data subject; and
- controller's obligations and rights.

The GDPR places far greater responsibility on processors for how they handle personal data from controllers than before. It is essential that processors have the appropriate operational and security arrangements in place to protect personal data. The best way to ensure that a processor is complying with their obligations under the GDPR is to conduct regular compliance checks. These checks should include:

- the level and content of the training the processor provides to their staff;
- the technical and organisational security measures in place; and
- whether the processor is complying with its specific legal obligations under the GDPR.

The DSP Toolkit requires Trusts to have a list of all the suppliers that handle personal data, the services or products they provide, their contact details and the duration of the contract. Also, all contracts with third parties who handle personal data must have been checked for compliance with Article 28 of GDPR.

What we found

Schedule 6(f) and Annex A of the NHS Standard Contract May 2018 and 2019/20 editions include all the terms and clauses required under GDPR. However, on inspection of sample contracts provided in evidence for our audits the NHS Standard Contract template was not used in all instances. This resulted in current contracts not including all the compulsory terms and clauses required under GDPR. In some cases, contracts pre-dated the advent of the GDPR and had not been updated to reflect the new requirements.

We had serious concerns about the lack of processor compliance checks being undertaken. Trusts were not conducting routine compliance checks to ensure that their processors had procedures in place to comply with their specific legal obligations under the GDPR. Compliance checks to assess completion of processor staff data protection training were also not carried out in most cases. Despite the NHS Standard Contract May 2018 and 2019/20 edition templates containing clauses to allow controllers the right to audit a processor's compliance, most of the Trusts had not inserted (or updated) any clauses within existing processor contracts giving them the right to undertake regular audits to ensure the processor is complying with their GDPR obligations.

In instances where there were the relevant clauses within contracts, there was not always evidence to support that these compliance checks had been carried out.

What we recommend

Trusts need to ensure that all written contracts with processors include all the necessary terms and clauses and that procedures are in place to ensure processor obligations under the GDPR are met. Where contracts pre-date the advent of the GDPR, they should undertake a full review of terms and clauses as a matter of urgency and update contracts to ensure compliance with data protection legislation.

Practical tip:
Keeping a central log of all processor or supplier contracts currently in place will provide more effective oversight and make it easier to schedule in regular reviews.

Trusts should conduct routine compliance checks to ensure that their processors have procedures in place to comply with their specific legal obligations under the GDPR. Compliance checks should include an assessment of their data security arrangements, processor staff data protection training and their awareness and understanding of data protection policies and procedures.

Practical tip:
Establishing a plan or programme for periodic reviews and compliance checks of all processors or suppliers will provide a framework of assurance to Trusts that the personal data shared and processed by third parties is done in a compliant manner.

For more information about what needs to be included in a data processor contract please visit our contracts section in the Guide to the GDPR.

Other development areas

We also noted procedures and practices in individual audits where, whilst not being systemic across all Trusts, we believe there was an opportunity to improve on current arrangements. We have commented on these below and made some suggestions on how they may improve them.

Observations	Suggestions
Fair processing information was not always made available for all groups, including children.	Trusts should make fair processing information for all groups accessible by a link on the Trust's website or have its own dedicated page. Trusts should put posters and paper copies in public and patient areas.
There were cases where operational staff's understanding or awareness of the Trust's fair processing information was not evident.	Trusts should ensure that staff are aware of the fair processing information relevant to their role or department as well as where to locate the information and how it can be provided to patients.
There were not always procedures in place to ensure that Data Protection Impact Assessments (DPIAs) are carried out prior to any type of processing which is likely to result in a high risk to individuals' interests or for any major new project involving the use of personal data.	Trusts should put clear DPIA procedures in place and staff should be made aware of this process and why it is important. They should encourage staff and give them resources to ensure that any new or major change to an existing system or process is put through a screening assessment to determine if a DPIA is required.
Several issues were identified regarding the disposal of confidential paper waste. There was evidence of confidential paper waste being stored in untied bags which are only collected when full and the use of unlocked confidential waste bins.	Trusts should store confidential paper waste securely until collected. This should be collected to a set schedule regardless of whether the bags are full. Trusts should always use and lock confidential waste bins.

Staff were not required to confirm at induction that they had read and understood key data protection policies.	Trusts should implement and monitor a sign-off process to ensure that all new staff are made aware of key data protection policies.
Information Asset Owners (IAO) and Information Asset Administrator (IAA) roles were not always formally assigned to appropriate staff and the role responsibilities were not clearly defined in job descriptions.	Trusts should ensure that IAOs and IAAs are appropriately assigned and are aware of their roles and responsibilities in the implementation of records management policy across all business areas. All IAOs and IAAs should complete training in a timely manner to help them carry out their responsibilities effectively.
Key Performance Indicators (KPIs) for several key areas such as subject access request performance, security breach information and records management were sporadically collated, and some Trusts did not collect any KPI information.	Trusts should ensure that they are monitoring their performance in key areas and that there is oversight of KPIs at Board level.

Good practice

There are some common areas where we noted that Trusts have measures in place to help them to comply with the legislation. These include:

- ✓ Established Information Management Steering Groups - which hold responsibility for providing general oversight for Information Governance and Data Protection compliance activity.

- ✓ Data Protection Forums - where operational staff can freely raise data protection issues. These forums have an escalation process to a central point to ensure that matters are resolved promptly.

- ✓ Weekly or monthly bulletins - to help disseminate and inform staff of new policies and subsequent updates.

- ✓ Location of policies - dedicated intranet areas where policies and procedures are made available for staff to view and read as required.

- ✓ Policy on Policies - policies, procedures and guidelines all written in an agreed format and styling, containing accurate version control and document change history.

- ✓ Governance frameworks - framework embedded into the structure of the organisation to support the data protection and information governance, records management and information management agendas.

- ✓ Published privacy information – information is typically provided online which explains the lawful basis for processing personal data and special categories of personal data.

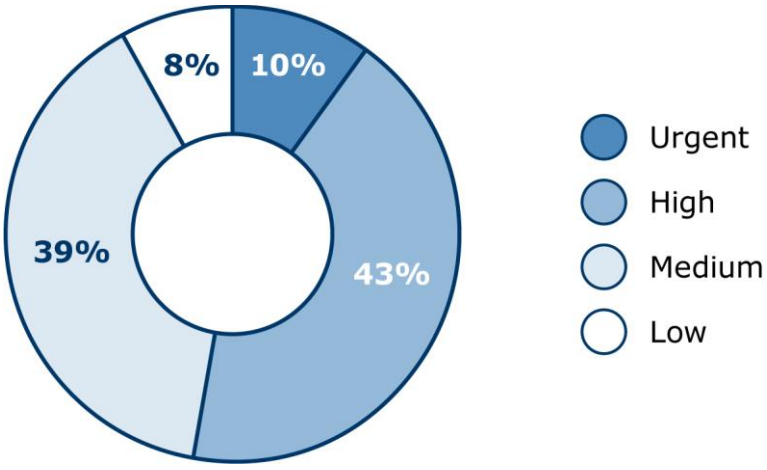
Recommendations made in our audits

Where we made recommendations, we assigned a priority to indicate the risk to data protection compliance if they are not implemented.

For example, an urgent priority rating was attached to recommendations addressing clear and immediate risks to the data controller's compliance with data protection legislation. High priority recommendations addressed risks which Trusts should tackle at the earliest opportunity to mitigate a breach of data protection legislation.

We made 312 recommendations across the 12 Trusts we audited, which included the following priorities:

- 32 'Urgent';
- 135 'High';
- 120 'Medium'; and
- 25 'Low' priority.



The above chart shows that many of the recommendations were a high priority. There was an average of 11 high priority recommendations made across the majority of Trusts. This is concerning because it means that most Trusts had significant issues that, whilst not imminent breaches, pose an increased risk of a Trust not complying with the governance and accountability principles of the GDPR.

Further reading

Data processor contracts	https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/contracts/
Data Protection Officer (DPO)	https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/
Privacy Notices	https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/ https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/
Record of Processing Activity	https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/ Referred to as 'Documentation' on our website.
Access to personal data	https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/
Previous audit reports	https://ico.org.uk/action-weve-taken/audits-advisory-visits-and-overview-reports/