Meeting the Requirements

Information Sharing

PECYN CYMORTH LLYWODRAETHU GWYBODAETH CYMRU

WELSH INFORMATION GOVERNANCE TOOLKIT

Introduction

Information Sharing, done in accordance with the law and good practice, can help organisations deliver modern, efficient services. Not sharing information can often lead to failing individuals who are in need, whether in urgent or longer-term situations. Over the years there have been many misunderstandings and barriers to sharing information, non-more so than with the arrival of the UK GDPR and the updated DPA in 2018. However, many of the requirements of data protection legislation place good practice for sharing information on a statutory footing.

Data protection law does not prevent information sharing if it is approached in a sensible and proportionate way. Whilst the UK GDPR and DPA have changed some aspects of data protection legislation, they do not prevent us from information sharing. Sharing information can bring benefits to the organisation and other organisations as well as patients and society in general. When done well it can benefit organisations in delivering modern, efficient services which better meet people's needs and make their lives easier.

For the purpose of this section 'information sharing' refers to examples such as:

- where the organisation provides another organisation with access to personal information on its clinical system. E.g. giving a hospital pharmacist access to GMP clinical systems to carry out medication reviews;
- several organisations pooling information and making it available to each other. E.g. when working within a Cluster, providing GPs from another Practice access to their patient records to provide treatment;
- sharing information on a routine, systematic basis for an established purpose. E.g. when working as part of a multi-disciplinary team.

See 'Table One' when considering sharing personal information. Please see the ICO's new 'Data sharing code of practice' for further information.

As we know personal information must be processed fairly and lawfully. For it to be considered fair, the organisation will need to explain to individuals how you will use their personal information and who you will share it with. The organisation should include this information in their privacy information, it should clearly explain the reasons why you are using their information including any disclosures or sharing. See the 'Right to be Informed' section for further guidance.

The organisation must be able to identify at least one lawful basis when sharing information and must be able to demonstrate that this has been considered prior to sharing, in order to satisfy the Accountability principle of UK GDPR. 'Table Two' sets out the lawful bases for processing, including the sharing of personal information.

The organisation will have appropriate security measures in place to protect information that is in transit; received by the organisation or transferred to another organisation. The organisation should have appropriate technical and organisational measures in place to protect personal data that you share. It is therefore important that the organisation sets out, and ensures compliance with, agreed levels of security when sharing personal information.

It is essential to provide appropriate training to staff that are likely to make significant decisions about data sharing or have access to shared data. The nature of the training will depend on their role within the sharing process. You can incorporate this into any training you already give on data protection, security, or legal obligations of staff.

Note: the 'Training and Awareness' pages provide further information.

All organisations have a common law duty of confidence as well as specific requirements under the UK General Data Protection Regulation (EU) 2016/679 and the Data Protection Act 2018 to ensure that confidential information is processed lawfully and protected from inappropriate disclosure.

Breach of confidence, inappropriate use of patient records or abuse of computer systems may lead to disciplinary measures for staff and the organisation. Although setting out the responsibilities of staff members will not automatically absolve the organisation of all blame, it will clearly be of assistance should a member of staff deliberately and intentionally, or recklessly, breach the law.

How do we reach Attainment Level 1?

Data sharing policies and procedures should be in place that clearly set out when it is appropriate for staff to share or disclose information. The organisations policies, procedures and guidance should set out how staff ought to respond to sharing requests. Any sharing of data must comply with the law, be fair, transparent and in line with the rights and expectations of the individuals whose data you are sharing. The policy should explain how you will achieve compliance with these requirements, for example, monitor information sharing logs, quality assess samples of instances of sharing.

Policies should also link in with your Data Protection Impact Assessment (DPIA) process, as you should carry out a DPIA on any information sharing that poses a high risk to the rights and freedoms of individuals. When considering information sharing the DPIA process will enable the organisation to consider their overall compliance with data protection legislation. As with all policies they should be proactively made available to staff.

Note: the 'Data Protection Impact Assessments' section provides further guidance.

The organisation should proactively take steps to only share the necessary personal information with processors or other third parties to achieve its specific purpose. When information is shared it should be pseudonymised or minimised wherever possible. You should also consider anonymisation, so the information is no longer personal data.

There will be circumstances when the organisation may consider it necessary to share personal information with other healthcare professionals, in order to provide additional healthcare services to its patients, where a contract is not in place or may not be the most appropriate arrangement. For example, providing an integrated service across a cluster network or delivering a specific multidisciplinary service. To enable this type of working there are a set of template information sharing documents which can be used to document the Data Controller responsibilities and set out a lawful and consistent approach to the sharing of information that will benefit the patient/service

users, while protecting the confidentiality of their personal information. See 'Table Three' for the ICO's expectations on data sharing agreements

It is good practice to have information sharing agreements in place when controllers share personal information. They set out the purpose of the data sharing, cover what is to happen to the data at each stage, set standards and helps all parties to be clear about their respective roles. They also help controllers and processors to demonstrate compliance and understand their obligations, responsibilities and liabilities.

These agreements can form part of the 'Wales Accord on the Sharing of Personal Information' (WASPI) framework. Organisations are therefore required to 'sign up' to the principal commitments set out in the Accord. Adopting the Accord will provide reassurance to other organisations and indeed the public that the organisation will treat personal information in a compliant manner and in-line with current legislation and good practice. It is essential that staff are made aware of the Accord and its supporting documentation. See 'Table Four' for further information on the Accord.

Staff should be made aware of and work to the Welsh Control Standard for electronic health and care records. This will provide re-assurance when working in a shared record environment, such as cluster working, and will enable the organisation to achieve compliance with statutory and legislative requirements for disclosing person identifiable information. See 'Table Five' for further information on the Control Standard.

'Table Six' sets out the ICO's expectations on data sharing agreements and 'Table Seven' details their expectations on data sharing policies and procedures. It is good practice to ensure that all staff accessing patient information/systems have undertaken Information Governance training within the last 2 years.

How do we reach Attainment Level 2?

The organisation should maintain a log of all the decisions made to share personal data and it should be reviewed regularly to obtain an overview of requests and outcomes.

The organisation should be able to justify the reasons why decisions to share specific personal data were made. Sharing should be lawful and comply with any statutory restrictions. In addition, the organisation must be able to establish the appropriate lawful basis for processing, as set out in data protection legislation. The organisation will also need to satisfy a separate condition if special categories of personal data are shared.

Health Boards and Trusts should deploy national Systems, such as NIIAS and AC3, to evidence the commitment to the Welsh Control Standard.

How do we reach Attainment Level 3?

Within the policy and procedures for information sharing, a process to ensure all Information Sharing Agreements in place are reviewed as necessary should be detailed. The process should

also outline the requirement for maintaining the Information Sharing Register in accordance with any changes.

Health Boards and Trusts should regularly report new and reviewed sharing agreements to the relevant Board/Committee to ensure appropriate governance and oversight.

Supporting Resources

ICO: Data Sharing Information Hub – *Provides clear guidance and practical tools for organisations and businesses on how to share data lawfully, while protecting people's personal information.*

ICO: Data Sharing Code of Practice – *Written to give individuals, businesses and organisations the confidence to share data in a fair, safe and transparent way. This code will guide practitioners through the practical steps they need to take to share data while protecting people's privacy.*

ICO: The Accountability Framework - *Accountability is one of the key principles in data protection law*

ICO: Data Protection by Design and by Default – *The UK GDPR requires you to put in place appropriate technical and organisational measures*

ICO: Children and the UK GDPR - *Practical guidance for organisations who are processing children's personal information*

Welsh Assembly Government: Confidentiality: Code of Practice for Health and Social Care in Wales - *This document sets out non-statutory guidance on best practice for those who work within or under contract to NHS or local authority social services authorities operating in Wales concerning confidentiality and the consent of patient and social care service users to the use of their health and social care records.*

General Medical Council: Confidentiality : Good Practice in Handling Patient Information 2018 - *Confidentiality (2018) sets out the principles of confidentiality and respect for patients' privacy that doctors are expected to understand and follow. Supplementary guidance explaining how these principles apply in situations doctors often encounter or find hard to deal with is also available*

The Wales Accord on the Sharing of Personal Information (WASPI) - *A framework to support organisations share personal information effectively and lawfully*

Welsh Control Standard for Electronic Health and Care Records - *The standard describes the principles and common standards that apply to systems that share electronic health and care records in Wales for the purpose of providing direct care.*

GOV.UK: Information: To Share or not to share? The Information Governance Review (2013) - *An independent review of how information about patients is shared across the health and care system.*

Summary Requirement

Attainment Level	Summary Requirement
1	Personal information is used and shared lawfully and relevant sharing principles of the Wales Accord on the Sharing of Personal Information (WASPI) and the common standards of the Welsh Control Standard for Electronic Health and Care Records have been adopted. All sharing is carried out in compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA)
2	**GMPs:** Where appropriate Information Sharing Protocols (ISPs) or Data Disclosure Agreements are recorded in from of an agreement register **Health Boards and Trusts:** Where appropriate Information Sharing Protocols (ISPs) or Data Disclosure Agreements are recorded in the form of an agreement register. National systems such as NIIAS and AC3 are used to demonstrate the adoption of the Welsh Control Standard for Electronic Health and Care Records
3	There is a review process in place to ensure agreements are kept up to date. Any changes or updates are reflected in the Information Sharing Register