Pecyn Cymorth Llywodraethu Gwybodaeth Cymru
Welsh Information Governance Toolkit

IGDC • DHCW

Expectations Guidance Document

1.6-Contracts and Information Sharing

Introduction

This guidance will provide basic information on what will be required from Organisation Administrators and Users to work through and complete the Contracts & Information Sharing section of the Welsh Information Governance Toolkit (WIGTK).

It is good practice for your organisation to have written data sharing agreements when the sharing of personal data happens. This helps all parties to understand the purpose for the sharing, what will happen at each stage and what responsibilities they have.

Written contracts are a legal requirement and help controllers and processors to demonstrate compliance and understand their obligations, responsibilities, and liabilities.

Having both in place will help your organisation to demonstrate compliance in a clear and formal way.

Minimum Expectations

Policies and Procedures
Senior Information Risk Owners (SIROs) and Information Asset Owners should ensure that information governance requirements in outsourced contracts meet the business needs of the organisation.

Article 28 of the UK GDPR makes written contracts between controllers and processors a requirement, therefore your organisation should have in place clear policies, procedures and processes that ensure appropriate contract controls are put in place, including appropriate information governance controls.

Your organisation's policies, procedures and guidance about data sharing should also include who has the authority to make decisions about systematic data sharing or one-off disclosures, and when it is appropriate to do so. It is essential all staff are aware of their responsibilities regarding data sharing and know how to carry them out effectively, and who to contact if they have queries.

Further information can be found in the ICO's Accountability Framework.

Documenting Contracts
Your organisation must document all sharing decisions for audit, monitoring, and investigation purposes, and be able to demonstrate that appropriate contracts and agreements are in place for all suppliers, contractors, data processors and third parties and that these are documented.

The necessary contract/agreement will vary depending on the relationship between the organisation and third party, these may include:

- Data Processing Agreements
- Joint Controller Agreements

Article 28 of the UK GDPR makes written contracts between controllers and processors a requirement:

“Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.”

Your organisation should keep a record of all contracts and agreements in place. These may be recorded within a specific contracts log or register or incorporated into the organisation's Record of Processing Activity (ROPA).

Pre and Post Procurement Checks – Not applicable to Third Party Contractors
Your organisation should be able to demonstrate that satisfactory checks proportionate to the risk of the processing have been conducted prior to agreeing any contracts with processors. This ensures third parties, contractors etc. who may process or have access to personal data on your behalf are compliant with data protection legislation, confidentiality and security requirements.

Due diligence checks may be conducted remotely or by visiting a third-party premises. The way in which checks are conducted is likely to depend on the proposed processing. For example, if the organisation were considering a third-party processor for offsite storage of records, it would be more appropriate to visit the premises in person to conduct these checks.

Due diligence checks may include:

- System Security checks (cyber security/encryption)
- Physical Security checks (access controls)
- Standards information (ISO/Cyber Essentials)
- Insurance information (cyber/breach)
- Previous data breaches / processes for managing a breach
- Risk management information
- Audit requests
- Employment standards (DBS checks)
- Business continuity plans

Article 28(1) of the UK GDPR says:

“Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.”

The ICO expects the organisation to conduct due diligence checks to guarantee that processors will implement appropriate technical and organisational measures to meet UK GDPR requirements.

The requirements for processor due diligence checks are set out within the Contracts and data sharing section of the ICO's Accountability Framework.

Secure Disposal
Your organisation should ensure that when confidential data is no longer required it is appropriately and securely disposed of. This applies to paper records, electronic records, and equipment such as old laptops, PCs, and mobile phones.

Where your organisation uses a third party to conduct its secure disposal, for example a shredding company or IT recycling organisation, it should have in place an appropriate contract that must include the requirement to have appropriate security measures in place and allow audit by your organisation.

Cyber Security Certification - Not applicable to GPs
Your organisation must ensure that any suppliers of IT systems have the relevant cyber security certification, ensuring that cyber security threats are considered when introducing suppliers into the NHS supply chain.

For example, external certification such as Cyber Essentials, or ISO27001, in line with Welsh Government Guidance and WHC 2017/025.

Standard Contracts and Clauses – HB/SHAs/Trusts and Prison Health only
The UK GDPR sets out specific terms that must be included in a contract, as a minimum.

The contract must state details of the processing and the obligations and rights of both the controller and the processor. It must also include the standards the processor has to meet when processing personal information on behalf of the controller.

Contracts must set out:

- the subject matter and duration of the processing,
- the nature and purpose of the processing,
- the type of personal data and categories of data subject, and
- the controller's obligations and rights.

Contracts must also include specific terms or clauses regarding:

- processing only on the controller's documented instructions,
- the duty of confidence,
- appropriate security measures,
- using sub-processors,
- data subjects' rights,
- assisting the controller,
- end-of-contract provisions, and
- audits and inspections.

See the ICO website for further information on 'controllers and processors'

Confidentiality Clauses for Staff
Processes should be in place to ensure confidentiality is always upheld by all staff members across your organisation, no matter what their level within the organisation is or their contractual status e.g., full time, temporary, locum etc.

Staff contracts should have the appropriate confidentiality clauses referencing data security and protection, with an emphasis on their duty to ensure the confidentiality and integrity of the data to which they have access.

Information Sharing Protocols/agreements – Not applicable to Third Party Contractors
When personal information is shared, both the disclosing and receiving organisations should have procedures in place that meet the requirements of law.

Your organisation should issue guidance that makes it clear to staff what the appropriate processes are and who best to contact regarding the sharing of data.

Procedures for sharing should be set out within an agreed information sharing protocol (ISP) or agreement. ISPs can be a useful way of providing transparency and assurance in respect of mutually agreed standards, including the lawful basis in which information is shared.

It should also be stated in the agreement the appropriate data handling if the agreement/contract were to end. For example, deletion of data, returning of data to the controller, etc.

Your organisation should maintain a log or register of all agreements/ISPs/contracts and ensure that these are reviewed and updated regularly, to confirm sharing remains appropriate.

Ad-hoc Sharing – Not applicable to Third Party Contractors
Throughout the course of its business, the organisation will receive ad-hoc requests for the sharing of personal information from other organisations.

The organisation should have a process in place for actioning these types of requests. Requests may come from a variety of parties, but often include:

- Police
- Local Authority
- Courts
- Research projects/initiatives

The organisation's process should include the consideration of the legal basis under UK GDPR as well as satisfying the requirements of the common law duty of confidentiality.

There are limited circumstances in which the common law duty of confidentiality can be overridden, these are:

- where the individual has capacity and has given valid informed consent
- where disclosure is in the overriding public interest
- where there is a statutory basis or legal duty to disclose, such as a court order or disclosure is supported by other legislation.

Wales Accord on the Sharing of Personal Information (WASPI) – HB/Trusts/SHAs, GPs and Prison Healthcare only
The WASPI Framework provides a practical approach to sharing personal information and provides common standards and templates for developing Information Sharing Protocols (ISPs) and Data Disclosure Agreements (DDAs).

The ICO's Data Sharing Code of Practice says:
"A data sharing agreement between the parties sharing and receiving data can form a major part of your compliance with the accountability principle of the UK GDPR. Sometimes a data sharing agreement is called an information sharing agreement, a data or information sharing protocol, or a personal information sharing agreement. It is good practice to have one in place."

The accountability principle requires organisations to take responsibility for what they do with personal data and show how they comply with the principles stated in Article 5(1) of UK GDPR.

Your organisation should be able to evidence its compliance and justify your approach to data sharing, so additional measures should be adopted, as necessary. A data sharing agreement would be one example of good practice to demonstrate your accountability. If you are unable to justify your approach, an accountability breach is likely.

For further information, templates and to sign up to WASPI, please visit the WASPI website.

Exceeded Expectations

This section is not required to be completed; however, it will help to further demonstrate your compliance and provide assurance.

These questions build on those you will have answered in the minimum expectations section; however, they are slightly more in depth.

Review processes
It is important that your organisation regularly reviews the contracts and any information sharing agreements/protocols that are in place to ensure they remain fit for purpose, and at the end of contract agreements, appropriate data handling occurs.

The review process should include contracts and agreements for suppliers, contractors, data processors and third parties.

Organisations should have an established review process in place to check all information sharing agreements remain up to date and that the Information Sharing Register is maintained and reviewed regularly.

The ICO's Data Sharing Code of Practice says:

"Under Article 30 of the UK GDPR, larger organisations are required to maintain a record of their processing activities. Therefore, you must ensure you document any data sharing you undertake, reviewing it regularly. Documenting this information is a practical way of taking stock of your data sharing. Knowing what information you have, where it is and what you do with it makes it much easier for you to comply with other aspects of the UK GDPR."

Reporting to senior management board – HB/SHAs/Trusts and Prison Health only
Your organisation should ensure that the Senior Management team or board are regularly sighted and updated on information sharing practices within the organisation.

They should be actively aware of data sharing agreements and protocols that are in place and maintain oversight of their management and when reviews are due.

Welsh Control Standard for Electronic Health and Care Records – HB/SHAs/Trusts and Prison Healthcare only
Health and social care organisations are developing closer links to deliver a strategic vision for transforming health and wellbeing services to the people of Wales. Delivering this vision relies on improved, secure access to electronic health and care records that are focussed on the individual; not the disease, service, or organisation where the care is being delivered.

Incremental progress is being made through a mixture of systems, software and national databases which make parts of the record available in different care settings. The complete record is likely to continue to be a combination of electronic and paper held in multiple organisations. This mixed landscape is likely to cover, but not be limited to:

- One organisation allowing another access to their healthcare systems. For example, GPs having access to a secondary care system.
- Multiple organisations contributing to a shared database. For example, the Welsh Results Reporting Service (WRRS).

By underpinning relevant national and local level policies and procedures the Control Standard aims to ensure broad consistency in the controls designed to ensure electronic health and care records are accessed and used appropriately. This should provide stakeholders with the reassurance that appropriate information governance and security measures are in place across Wales.

The Control Standard aims to compliment the conditions, obligations and requirements set out in the Wales Accord on the Sharing of Information (WASPI) framework. Where WASPI agreements are purpose focused, the Control Standard focuses on the system used to share the information to deliver effective public services.

Adopting the standards will help ensure that your organisation is working in a shared record environment is compliant with statutory and legislative requirements for disclosing personal identifiable information in line with the Data Protection Act 2018 (DPA), the UK General Data Protection Regulation (UK GDPR) (EU) 2016/679 and common law duty of confidentiality.

Further information on the Welsh Control Standard for Electronic Health and Care Records is available on the Information Governance website.