Health Information and Quality Authority

An tÚdarás Um Fhaisnéis agus Cáilíocht Sláinte

GUIDE TO THE ASSESSMENT JUDGMENT FRAMEWORK

National Standards for Information Management in Health and Social Care

Safer Better Care

About the Health Information and Quality Authority

The Health Information and Quality Authority (HIQA) is an independent statutory body established to promote safety and quality in the provision of health and social care services for the benefit of the health and welfare of the public.

Reporting to the Minister for Health and engaging with the Minister for Children, Equality, Disability, Integration and Youth, HIQA has responsibility for the following:

- **Setting standards for health and social care services** — Developing person-centred standards and guidance, based on evidence and international best practice, for health and social care services in Ireland.

- **Regulating social care services** — The Chief Inspector of Social Services within HIQA is responsible for registering and inspecting residential services for older people and people with a disability, and children's special care units.

- **Regulating health services** — Regulating medical exposure to ionising radiation.

- **Monitoring services** — Monitoring the safety and quality of permanent international protection accommodation service centres, health services and children's social services against the national standards. Where necessary, HIQA investigates serious concerns about the health and welfare of people who use health services and children's social services.

- **Health technology assessment** — Evaluating the clinical and cost effectiveness of health programmes, policies, medicines, medical equipment, diagnostic and surgical techniques, health promotion and protection activities, and providing advice to enable the best use of resources and the best outcomes for people who use our health service.

- **Health information** — Advising on the efficient and secure collection and sharing of health information, setting standards, evaluating information resources and publishing information on the delivery and performance of Ireland's health and social care services.

- **National Care Experience Programme** — Carrying out national service-user experience surveys across a range of health and social care services, with the Department of Health and the HSE.

Overview of the health information function of HIQA

Good information is the foundation of a high-quality health and social care service. As part of a person's journey through the health and social care system, information is collected and shared at different stages and used to inform their care. This is known as the primary use of information. High-quality data is also important for other purposes such as planning and managing services, policy-making, research and innovation. For example, information may be used to decide where to locate a new service or to understand how practice can be changed to improve a person's experience of care. This is known as the secondary use of information.

Whether used for primary or secondary purposes, it is essential that information is managed effectively and securely and used to its full potential to promote safer better care, improved outcomes and overall wellbeing for people using services. A human rights-based approach should be of central importance and seek to balance the rights of people with the broader societal value of using health and social care information. A strategic and coordinated approach that is aligned with information standards is also essential to ensure data is captured and managed in line with best practice. A well-embedded standards-based information environment will allow all stakeholders, including the general public, patients and service users, health and social care professionals and policy-makers, to make choices or decisions based on the best available information.

Digital health, which is the use of digital technologies to improve health, is critical to ensuring that information is available when and where it is required. An effective digital health infrastructure can support the secure, effective transfer of information by ensuring information is captured in the right format so that it can be shared easily and securely across services. The necessary information should be accessible by all health or social care professionals providing care and to the person it relates to. This will lead to more efficient and effective delivery of care and ensure people do not have to provide the same information on multiple occasions.

The Health Information and Quality Authority (HIQA) has responsibility for setting standards for all aspects of health information and monitoring compliance against those standards, as set out in Section 8(1) of the Health Act 2007.(1) Under the Act, HIQA is also charged with evaluating the quality of the information available on health and social care and making recommendations to the Minister and the Health Service Executive (HSE) in relation to improving the health information system. Through its health information function, HIQA also plays a key role in providing evidence to inform national health information policy and shape the health information landscape in Ireland. HIQA works to ensure that high-quality health and social care information is available to support the delivery, planning and monitoring of services which in turn ensures safer better care for all.

Table of Contents

1 Introduction

Data and information are generated in huge volumes everyday across the health and social care system. Although health and social care information is an extremely valuable resource, there are significant costs associated with its management in terms of how it is collected, used and shared. Therefore, it is imperative that organisations have appropriate structures, systems, policies and procedures in place which are aligned with evidence-based standards. This will ensure that information collected is of the highest quality and used to its full potential to promote safer better care, improved outcomes and overall wellbeing.

The aim of the *National Standards for Information Management in Health and Social Care* (referred to as national standards in this document) is to contribute to safer better care by improving the management of health and social care information. They complement other health and social care standards which have been developed by HIQA.

The *National Standards for Information Management in Health and Social Care* should be reviewed in advance of reading this guide.

1.1 Purpose of the Guide to the Assessment Judgment Framework

This document was developed as part of a suite of resources to support the implementation of the national standards, to include:

- **The Assessment Judgment Framework**
- Guide to the Assessment Judgment Framework
- Self-assessment tool

National Standards for Information Management in Health and Social Care	**Assessment Judgment Framework**	**Guide to the Assessment Judgment Framework**	**Self-assessment tool**
	Sets out lines of enquiry to assist organisations and HIQA reviewers in assessing and making judgments on compliance with the standards.	Provides detailed guidance for organisations and HIQA reviewers about how compliance with the national standards will be assessed and how each standard can be met. Used alongside the Assessment Judgment	Helps organisations determine the extent to which they comply with the standards and identify areas of good practice and where improvement is needed.

		Framework when assessing compliance.	

2 Assessing compliance

2.1 Reviews

In line with its legislative remit, HIQA carries out reviews in order to assess compliance with the national standards. Review methodology is updated periodically, but in general, includes the following steps:

1. The organisation is notified of the review
2. A self-assessment tool and a request for documents are sent to the organisation
3. Site visits take place
4. All information and evidence is collated and analysed and used to make judgments on compliance (see section 2.2)
5. Report and recommendations are drafted
6. The draft report is sent to the organisation for factual accuracy review and right of reply
7. The report is updated based on feedback received from the organisation
8. Following approval, the report is published online.

2.2 Judgments on compliance

In order to make judgments about compliance, HIQA will:

- review data and documents obtained from the organisation prior to, and during, the site visit(s)
- communicate with management and staff from the organisation to gain an understanding of information management within the context of their organisation and the services that they deliver, in order to ascertain if their experiences reflect what is contained in the documents reviewed. Discussions may also focus on their experiences and training.

When reviewers have gathered sufficient information, they will assess the information to make a judgment on the level of compliance with the relevant standard.

There are four levels of compliance, outlined in **Table 1**. We term them ‘judgment descriptors’, and they are used to describe how an organisation performed against each of the standards.

Table 1 Judgment descriptors

Compliant	A judgment of compliant means that the organisation was in compliance with, or exceeded, the requirements of the relevant standard.
Substantially compliant	A judgment of substantially compliant means that the organisation met most of the requirements of the relevant standard, but some action is required to be fully compliant.
Partially compliant	A judgment of partially compliant means that the organisation meets some of the requirements of the relevant national standard while other requirements are not met.
Not compliant	A judgment of non-compliant means that one or more findings indicate that the relevant national standard is not being met, and immediate action is required by the organisation to mitigate the impact of the non-compliance.

3 Structure of the guidance on each principle

The national standards comprise three elements: principles, standards and features. In this guide, each principle and the associated standards are described over five sections, as follows:

1. **An introduction to the principle:** This section provides a brief overview of what the principle is and places it within the context of information management.

2. **The standards associated with the principle:** This section outlines the standard statements associated with each principle. For the full list of features which accompany each standard statement, see the national standards document which is available at www.hiqa.ie.

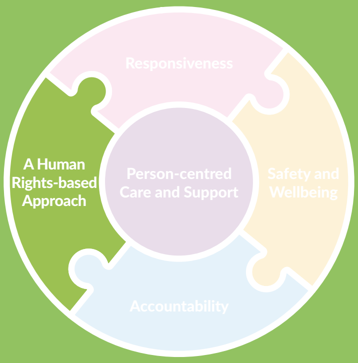
3. **A description of what an organisation meeting the principle looks like:** This section describes a compliant organisation and how an organisation might meet the standards under the principle. Where a standard has been complied with, it is the responsibility of organisations to seek out ways to continuously improve the quality of their service.

4. **Examples of the sources of information and evidence that are reviewed to assess compliance with each standard:** This section gives examples of the information and evidence that are reviewed to assist with assessing compliance. The examples are listed under the headings of documentation, communication and observation. While not intended to be an exhaustive list, these examples are provided to support organisations in achieving compliance with the standards and to assist reviewers in planning for a review, gathering information, and making judgments about compliance**.**

5. **Examples of indicators that demonstrate the organisation's level of compliance with each standard:** This section outlines examples of the type of findings that could demonstrate evidence of compliance and non-compliance. The examples detailed are not an exhaustive list but are there to assist in determining the levels of compliance.

Principle 1

A human rights-based approach


Responsiveness
A Human Rights-based Approach
Person-centred Care and Support
Safety and Wellbeing
Accountability

Guidance on Principle 1: A human rights-based approach

An introduction to the principle

In the context of information management, a human rights-based approach should seek to balance the protection and rights of people with the broader societal value of data use for health.[4,5] This can only be achieved by evaluating information management practices to identify and mitigate any potential harms which may occur at an individual, group or community level (such as a loss of privacy or a risk to public health).[5] Organisations should also promote an inclusive, sensitive and equitable approach to information management. An organisation adopting a rights-based approach in the context of health information should ensure:

- transparency regarding how and why data is collected, used and shared and that peoples' will and preferences are reflected in decisions regarding how information is managed and governed.
- privacy and confidentiality of a person's personal information and medical records is maintained in line with data protection legislation.

The standards associated with the principle

Principle 1: A human rights-based approach	
Standard 1.1 Uphold people's rights relating to information	
What a person should expect: I am confident that arrangements are in place to promote and uphold my rights relating to information and I fully understand how and why the organisation collects, uses and shares my information.	**What an organisation should do to achieve this:** The organisation has effective arrangements in place to ensure a person's rights under relevant legislation are promoted and upheld, balancing these rights against other values, fundamental rights, human rights, or legitimate, public or vital interests. The organisation is transparent about how and why it collects, uses and shares information.
Standard 1.2 Protect privacy and confidentiality	
What a person should expect: I am confident that the organisation will protect my privacy and confidentiality when collecting, using and sharing my information.	**What an organisation should do to achieve this:** The organisation has effective arrangements in place to protect the privacy and confidentiality of people about whom it collects, uses and shares information.

A description of what an organisation meeting this principle looks like

In a well-run organisation, all human rights, including human rights relating to data and information, are protected, promoted and upheld. While protection against data-related harm and violations falls within the remit of general data protection legislation, health and social care information requires additional specialised protections in both legislation and in organisations' information management practices. In order to adopt a human rights-based approach, an organisation should be strategic and forward-thinking in developing and implementing information management policies and procedures that are aligned with current and forthcoming legal frameworks and human rights treaties.(6,7)

An organisation adopting a human rights-based approach to health information is fully transparent with regard to what information it collects about people and how it uses and shares it. This may take the form of a privacy statement that is made publically available in an accessible format (for example, on the organisation's website) and updated regularly as needed. Central to a human rights-based approach to data and information is taking steps to ensure that the collection of data is limited to what is necessary. This is particularly relevant for sensitive health and social care information which must only be collected when necessary to achieve a specific and justifiable objective. Closely linked to this, organisations must have arrangements in place to ensure that access to personal health and social care information for staff is on a strict need-to-know basis.

An organisation adopting a human rights-based approach to health information is also fully transparent about what people's rights are in relation to the information it collects about them, and the choices they have with regard to this information. These rights include, but are not limited to: right of access, right to be informed (transparency), right to rectification, right to erasure, right to data portability, right in relation to automated processing, right to object to processing, and right of restriction.(7) Transparency about rights is inherent to informed consent, and a well-run organisation has arrangements in place to ensure full transparency with regard to all potential uses of information, and the procedures for facilitating people's consent preferences to be captured and changed, where relevant.

An organisation adopting a human rights-based approach to health information evaluates and assesses risks relating to information management on a regular basis in order to identify and mitigate potential harm at every stage of the data and information lifecycle. This could include undertaking Data Protection Impact Assessments (DPIAs) for both new and ongoing protects. In a well-run organisation, all practices associated with the collection, use and sharing of health information are planned in such a way that potential risks are mitigated. This continues to be relevant even in the context of information that is not personally-identifiable.

Importantly, organisations should seek to balance the protection and rights of people with the broader societal value of data use for health. Achieving such a balance requires a coordinated approach to risk assessment to identify and mitigate potential harms, such as data breaches, at all stages of the data and information lifecycle.

Following a human rights-based approach to health information means that management and staff at an organisation recognise the importance of ensuring equitable representation of individuals, groups and communities in the data, regardless of social or economic characteristics, as well as the need to promote equitable sharing of the value created by the use of the data. This includes the consideration of data collection and reporting methodologies and processes which are inclusive and consider the demographic and social attributes of the people about whom the information relates.(5) As such, an equitable approach to information management should be inherent in a well-run organisation and central to decisions regarding data collection and use of information.

Sources of evidence for standards within Principle 1

Through review of documents obtained from the organisation prior to, and during, the site visit, reviewers may:

- Investigate if the organisation is transparent about what information it collects, why it collects it, and how it uses it (for example, in the form of a privacy statement published on the organisation's website).
- Explore whether the organisation is transparent about what people's rights are in relation to the information it collects about them and the choices they have about this. This includes a person's right to access, right to be informed, right to rectification, right to erasure, right to object, right in relation to automated processing, right to restriction and right to data portability.
- Examine what arrangements the organisation has in place to ensure people's rights relating to their data, including privacy, are respected and upheld (including policies and procedures and arrangements for staff training in this area).
- Identify what arrangements are in place to ensure policies and procedures with regard to informed consent are appropriate, including the procedures around obtaining informed consent for using information for specific purposes and for facilitating people to change their consent preferences.
- Find out how feedback on data rights, including complaints, is submitted and subsequently reviewed by the organisation (including the suitability of arrangements in place to submit feedback), and how frequently changes to information management practices are implemented based on feedback.
- Find out how data protection risks are identified and mitigated against.
- Identify if local and regional policies and procedures are aligned to national policy.
- Support the identification of additional lines of enquiry for the review.

Documents reviewed could include:

- Policies and procedures (covering areas such as privacy and confidentiality; data requests; document and records management; data breach management; and data security).
- Privacy statements (or notices)
- Data Protection Impact Assessment reports and summaries

- Staff training records and training materials
- Audit records
- Organisational charts
- Guidance for people (including posters, leaflets, website content).

HIQA reviewers will communicate with the organisation, and in some situations, observe practice, to:

- Get clarification and further detail regarding any queries that arise through the review of documentation obtained from the organisation.
- See how aware staff are of people's rights relating to the information the organisation collects about them, and how they ensure relevant rights are upheld and promoted.
- Identify whether roles and responsibilities regarding people's rights relating to their information are clearly outlined to staff, if adequate training in this area is available for staff, and if specific information governance roles are in place and adequately communicated across the organisation.
- Explore whether policies, procedures and practices are in place within the organisation to support an equitable and inclusive approach to information management.
- Understand how data holders, owners and users are supported to make decisions about data and information.
- Identify what legal frameworks underpin policies and procedures relating to data rights.
- Understand how measures to ensure privacy and confidentiality are implemented by the organisation.

This communication and observation could take the form of:

- Telephone, teleconference, and email contact prior to, and following, the site visits
- Online or in-person meetings, interviews, and focus groups
- System demonstrations and observations of practice.

Indicators of compliance

Standard 1.1: Uphold people’s rights relating to information	
Indicators of compliance include:	▪ Evidence of a coordinated approach to the development and implementation of clear policies and procedures that are reflective of a human rights-based approach, leading to standardised practices across the organisation. ▪ Evidence that staff roles and responsibilities with regard to upholding and promoting people’s rights are documented and communicated, with high levels of awareness among staff working across the organisation. ▪ Publicly-available information on what people’s rights and choices are with regard to the information the organisation collects about them. ▪ Evidence that information is collected, used and shared in such a way that respects the diversity of people about whom it relates. ▪ Evidence of a coordinated approach to reviewing, auditing and updating relevant policies and procedures.
Indicators of substantial compliance include:	▪ Policies, procedures and practices are reflective a human rights-based approach overall, but there is some evidence of gaps in existing policies and procedures, leading to some variation in practices. ▪ Good levels of awareness among staff overall but there is evidence of gaps in staff knowledge relating to some rights and choices relating to people’s information, and their roles and responsibilities relating to upholding and promoting rights. ▪ Publicly-available information on some, but not all, rights and choices people have with regard to the information the organisation collects about them. ▪ Evidence that relevant policies and procedures are reviewed and updated periodically but audited only on an ad hoc basis.
Indicators of partial compliance include:	▪ Policies lack detail with regard to people’s rights and choices relating to their information and procedures are inconsistently implemented across the organisation. ▪ Varying levels of awareness amongst all staff with regard to people’s rights and choices relating to their information, and their roles and responsibilities relating to upholding and promoting rights.

	▪ Evidence that relevant policies and procedures are reviewed and updated on an ad hoc basis but not routinely audited.
Indicators of non-compliance include:	▪ Policies, procedures and practices are not reflective of a human rights-based approach and there is evidence of variation in practices across the organisation. ▪ Low levels of awareness among all staff with regard to people's rights and choices relating to their information, and their roles and responsibilities relating to upholding and promoting rights. ▪ No publically available information on people's rights and choices with regard to the information the organisation collects about them. ▪ Evidence that relevant policies and procedures are not reviewed, audited or updated regularly.

Standard 1.2: Protect privacy and confidentiality	
Indicators of compliance include:	▪ Evidence of a coordinated approach to the development and implementation of clear policies and procedures, leading to standardised practices across the organisation with regard to protecting people's privacy and confidentiality. ▪ Evidence that staff roles and responsibilities with regard to protecting people's privacy and confidentiality are documented and communicated, with high levels of awareness among staff working across the organisation. ▪ Identifiable individual(s) with responsibilities with regard to data protection and information governance (including a Data Protection Officer). ▪ The publication and regular review of privacy statements. ▪ Evidence that DPIAs are conducted for defined projects, as required; that the findings of DPIAs are used to mitigate against any data protection risks and implement necessary changes; and that DPIA reports or summaries of them are published, as appropriate. ▪ Evidence of a coordinated approach to reviewing, auditing and updating relevant policies and procedures.
Indicators of substantial compliance include:	▪ Policies, procedures and practices protect people's privacy and confidentiality overall, but there is some evidence of gaps in existing policies and procedures, leading to some variation in practices. ▪ Good levels of awareness among staff overall but there is evidence of gaps in staff knowledge relating to protecting privacy and confidentiality, and their roles and responsibilities relating to this. ▪ At least one identifiable individual has responsibilities relating to data protection and information governance; however, the roles are not formalized and/or some gaps are evident. ▪ DPIAs are conducted for most projects that involve the processing of personal data and DPIA reports or summaries are published as appropriate, but there is evidence that the findings with regard to identified risks are not always fully implemented in order to mitigate against those risks. ▪ Evidence that relevant policies and procedures are reviewed and updated periodically but audited only on an ad hoc basis.

Indicators of partial compliance include:	▪ Policies lack detail with regard to people's privacy and confidentiality and procedures are inconsistently implemented across the organisation. ▪ Varying levels of awareness amongst all staff with regard to protecting people's privacy and confidentiality, and their roles and responsibilities relating to this. ▪ A privacy statement is available but there is evidence that it is not regularly reviewed or updated. ▪ DPIAs are conducted for a minority of projects but gaps are evident in terms of how comprehensive they are, how the findings are implemented, and how accessible they are (reports or summaries not published). ▪ Evidence that relevant policies and procedures are reviewed and updated on an ad hoc basis but not routinely audited.
Indicators of non-compliance include:	▪ Current policies, procedures and practices do not clearly demonstrate how the organisation protects the privacy and confidentiality of people about whom information is collected. ▪ Low levels of awareness among all staff with regard to protecting people's privacy and confidentiality, and their roles and responsibilities relating to this. ▪ No identifiable individuals with responsibilities relating to data protection and/or information governance. ▪ No privacy statement available. ▪ No evidence of DPIAs being conducted. ▪ Evidence that relevant policies and procedures are not reviewed, audited or updated regularly.

Principle 2

Safety and wellbeing

Responsiveness
A Human Rights-based Approach
Person-centred Care and Support
Safety and Wellbeing
Accountability

Guidance on Principle 2: Safety and wellbeing

An introduction to the principle

Within the context of information management, the principle of safety and wellbeing refers to an organisation promoting a culture of safety by ensuring information is available in the right form, in the right place and at the right time, with the appropriate safeguards in place. In addition, information collected as part of routine care should be effectively used for secondary purposes to continuously drive improvements in safety and wellbeing. The benefits of using information effectively, for both primary and secondary use, include:

- improving people's health outcomes
- improving people's experiences of using health and social care services
- reducing waste through the avoidance of unnecessary repeat tests and procedures
- generating knowledge through clinical audit and research and continuously applying learnings to improve services
- identifying and monitoring epidemiological trends
- enhancing staff education, training and performance.

The standards associated with the principle

Principle 2: Safety and wellbeing	
Standard 2.1: Optimise the accessibility, use and value of information	
What a person should expect: I am confident that my information is used, in line with legislation and innovation, to continuously drive improvements in care, safety and wellbeing.	**What an organisation should do to achieve this:** The organisation has effective arrangements in place to use data and information as a resource in the planning, delivering and management of care and in the improvement of safety and wellbeing in line with legislation, national digital health policies and strategies, and emerging and evolving technologies.
Standard 2.2 Undertake effective stakeholder engagement	
What a person should expect: I am confident that the organisation engages with all relevant stakeholders, including people using services, members of the public and professionals, to identify their priorities and expectations in terms of information management and in getting access to information to inform decisions about care, support and wellbeing.	**What an organisation should do to achieve this:** The organisation has effective arrangements in place to promote a strategic approach to engaging with key stakeholders, including people using services, members of the public and professionals, in order to identify current and future needs for information management including providing access to information and the associated system design and requirements to inform decisions about care, support and wellbeing.

A description of what an organisation meeting this principle looks like

All health and social care organisations should strive to deliver safer better care and recognise that high-quality information and effective information management practices are central to achieving this goal. High-quality health and social care information has the potential to improve patient outcomes by facilitating better clinical decision-making. It also enables services to be planned and managed more effectively, informs policy-making, accelerates research, and drives innovation.

For an organisation to ensure information is available in the right form, in the right place and at the right time for all potential users, including members of the public, it must have effective arrangements in place. Such arrangements include having policies and associated procedures, including appropriate safeguards to facilitate access to one’s own information. It also includes having the necessary policies and procedures with regard to information-sharing within, and across, organisations to support timely clinical decision-making. In emergency situations, timely access to reliable and accurate information can save lives. It can also reduce burden on patients and enhance health system efficiency through the avoidance of unnecessary repeat tests and procedures.

An organisation must also be aware of, and adequately resourced to meet, its reporting obligations. Data collected everyday across health and social care organisations, such as data on waiting lists, inpatient activity, incidents, and costs, is collated and shared for secondary use purposes including national reporting and performance monitoring. This information is also subsequently used for planning and management purposes, evaluating the quality and safety of services, research, and policy-making. An organisation that recognises the role information plays in promoting safety and wellbeing strives to ensure that effective arrangements are in place to optimise the accessibility, use and value of the information it collects and reports.

The sharing, use and re-use of information are essential to creating value from it; however, the effective sharing and use of information are reliant on adequate technical infrastructure. A well-run organisation strives to effectively use all available resources and infrastructure, including ICT equipment and software, for the collection, use and sharing of information. It is strategic and proactive in ensuring it aligns with all national digital health policies and strategies and broader developments in the sector. The use of a unique identifier to avoid duplication and misidentification of individuals is recognised as a key driver of patient safety and is also essential for the effective use of data for secondary purposes, and ultimately fundamental to good information management. Organisations must ensure they have a method of uniquely identifying all individuals and should align with national policy in this area, including the implementation of the Individual Health Identifier, once available.

The sharing of information is associated with additional risks, so organisations must endeavour to identify and mitigate all risks at every stage of the process. A well-run organisation has plans in place to ensure business continuity and continuity of care in the occurrence of an event, such as a data breach or cyber-attack, which impacts on the accessibility of systems.

An organisation that recognises the importance of promoting the use of its information to improving safety and wellbeing takes a strategic approach to engaging with key stakeholders. All stakeholders, including people about whom the organisation collects information, should be engaged in the design, development and continual improvement of health information systems. Within the context of safety and wellbeing, meaningful engagement ensures that all stakeholders are given the opportunity to express their will and preferences about the information that the organisation holds and are included in the planning, management and design of initiatives and systems to optimise the accessibility, use and value of information.

Meaningful engagement with all stakeholders, including members of the public, is essential to achieving the balance between protecting the rights of people with the broader societal value of data use for health. Such engagement is essential to enhance and strengthen people's trust in the processes surrounding the use and sharing of their information.

Sources of evidence for standards within Principle 2

Through review of documents obtained from the organisation prior to, and during, the site visit, reviewers may:

- Investigate what policies and procedures are in place to facilitate and optimise the use and sharing of information internally and externally in line with relevant legislation and reporting obligations.
- Investigate if the organisation takes a strategic approach to engaging with all key stakeholders about information management practices.
- Explore whether existing practices regarding the use and sharing of information are aligned with national digital health initiatives, policies and strategies (including the use of unique identifiers and safe data linkage) and emerging and evolving technologies (such as web-based tools, business intelligence and artificial intelligence).
- Explore whether processes are in place to ensure risks relating to information sharing are assessed and managed appropriately.
- Find out if data sharing rules and guidelines are in place.
- Investigate if adequate plans are in place to respond to an event which impacts on the accessibility or use of information.
- Explore whether information is being used to support the development of a learning health system.
- Identify if local and regional policies and procedures are aligned to national policy.
- Support the identification of additional lines of enquiry for the review.

Documents reviewed could include:

- Reports, including annual reports, business plans, strategic plans
- Policies and procedures (covering areas such as data requests; data sharing rules; data access levels; disaster recovery; risk assessment; and data linkage)
- Records of the organisation’s routine reporting obligations (and any associated policies and procedures)
- Records of any stakeholder engagement undertaken or planned.

HIQA reviewers will communicate with the organisation, and in some situations, observe practice, to:

- Get clarification and further detail regarding any queries that arise through the review of documentation obtained from the organisation.
- Explore whether policies and procedures with regard to information sharing are optimal from the perspectives of staff working within the organisation.
- Explore staff experiences and perceptions on the availability of ICT resources and infrastructure.
- Find out if staff are aware of the latest technologies with regard to information management, as well as relevant digital health policy and strategies.
- Examine if staff are aware of data sharing rules and guidance, and clear about their role in terms of managing associated risks.
- Understand staff experiences and views of stakeholder engagement for the purposes of identifying individuals' priorities and expectations in terms of information management.

This communication and observation could take the form of:

- Telephone, teleconference, and email contact prior to, and following, the site visits
- Online or in-person meetings, interviews, and focus groups
- System demonstrations and observations of practice.

Indicators of compliance

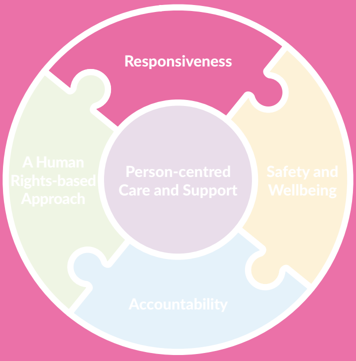
Standard 2.1: Optimise the accessibility, use and value of information	
Indicators of compliance include:	▪ Evidence of a coordinated approach to the development and implementation of clear policies and procedures to ensure high-quality information is available to all stakeholders and that practices are standardised across the organisation. ▪ Evidence that staff roles and responsibilities with regard to the use and sharing of information are documented and communicated, with high levels of awareness among staff working across the organisation. ▪ Strategic use of ICT resources and infrastructure to optimise the accessibility and use of information for both primary and secondary uses. ▪ Advanced systems and practices with regards to the use of available digital health initiatives and technologies, in line with national and international developments. ▪ Alignment with national policy, standards and best practice in key areas such as use of unique identifiers and data linkage ▪ Evidence of a standardised and coordinated approach to the assessment and management of risks associated with information sharing. ▪ Evidence that information is being used to support the development of learning health systems. ▪ Routine monitoring of how information is used in order to identify areas for improvement. ▪ Evidence of a coordinated approach to reviewing, auditing and updating relevant policies and procedures.
Indicators of substantial compliance include:	▪ Policies, procedures and practices optimise the accessibility, use and sharing of information overall, but there is evidence of areas for improvement in some instances (for example, in how individuals are facilitated to access their own health and social care records, or the availability of information for secondary uses). ▪ Good levels of awareness among staff overall but there is evidence of gaps in staff knowledge relating to some aspects of the use and sharing of information, and their roles and responsibilities relating to this.

	▪ Evidence of some progress with regard to the use of ICT resources and infrastructure, the adoption of digital health initiatives and technologies, and alignment with national policy and standards and best practice in this area. ▪ Evidence that relevant policies and procedures are reviewed and updated periodically but audited only on an ad hoc basis.
Indicators of partial compliance include:	▪ Policies lack sufficient detail to optimise the accessibility, use and sharing of information, and procedures are inconsistently implemented across the organisation. ▪ Varying levels of awareness amongst all staff with regard to the use and sharing of information, and their roles and responsibilities relating to this. ▪ Evidence of some initial attempts to improve its use of ICT resources and infrastructure and to align with digital health initiatives and technologies; however, practices remain underdeveloped overall. ▪ Inconsistent approach to assessing and managing risks associated with information sharing. ▪ Evidence that relevant policies and procedures are reviewed and updated on an ad hoc basis but not routinely audited.
Indicators of non-compliance include:	▪ Policies, procedures and practices do not optimise the accessibility, use and sharing of information, and there is evidence of variation in practices across the organisation. ▪ Low levels of awareness among all staff with regard to the use and sharing of information, and their roles and responsibilities relating to this. ▪ Information sharing is constrained by a lack of adequate ICT infrastructure and other resources and an over-reliance on paper-based systems. ▪ No alignment with national policy, standards and best practice in key areas such as use of unique identifiers and data linkage. ▪ No routine assessment or management of risks associated with information sharing. ▪ Evidence that relevant policies and procedures are not reviewed, audited or updated regularly.

Standard 2.2: Undertake effective stakeholder engagement	
Indicators of compliance include:	▪ Evidence of a planned and coordinated approach to stakeholder engagement across the organisation. ▪ Evidence of stakeholder mapping being undertaken to ensure all key stakeholders are identified, and stakeholder plans being developed (for example, documented stakeholder mapping exercises and stakeholder plans). ▪ Evidence that stakeholder engagement has informed relevant policies and procedures, outputs (such as reports), and health information initiatives or systems. ▪ Established and active learning communities.
Indicators of substantial compliance include:	▪ Evidence that some stakeholder mapping and engagement have been undertaken to inform policies and procedures, but the overall approach to stakeholder engagement is somewhat uncoordinated, with gaps apparent in terms of how stakeholders are identified and how stakeholder plans are developed. ▪ Evidence of some gaps in how the findings of stakeholder engagement are implemented.
Indicators of partial compliance include:	▪ Evidence of minimal stakeholder mapping and engagement being undertaken, with key groups excluded. ▪ Evidence of limited implementation of the findings of stakeholder engagement.
Indicators of non-compliance include:	▪ A lack of evidence to demonstrate that any stakeholder engagement (including stakeholder mapping or planning) has been undertaken. ▪ Evidence that policies and procedures relating to information management, outputs (such as reports), and health information initiatives or systems have been developed without the involvement of key stakeholders.

Principle 3

Responsiveness


Responsiveness
A Human Rights-based Approach
Person-centred Care and Support
Safety and Wellbeing
Accountability

Guidance on Principle 3: Responsiveness

An introduction to the principle

In the context of health and social care information, the principle of responsiveness relates broadly to organisations responding to, and meeting the needs of, people using services and the health and social care system as a whole. In terms of information management, a responsive organisation ensures its practices are aligned with national and international best practice, drives innovation through the adoption of emerging technologies, and promotes the effective and safe use of high-quality information to ensure maximum benefit is achieved.

The standards associated with the principle

Principle 3: Responsiveness	
Standard 3.1 Align with best practice regarding data standards and agreed definitions	
What a person should expect: I am confident that my information is collected and managed so it can be shared across organisations to ensure it is meaningful, accurate and available when needed to inform good decision-making.	**What an organisation should do to achieve this:** The organisation has effective arrangements in place to align with the latest national and international standards, policies, guidance and recommendations for safe and effective collection, use, and sharing of information, and it strives to drive innovation in its information management practices to ensure good quality data is available when and where it is needed.
Standard 3.2 Enhance data quality	
What a person should expect: I am confident that my information is accurate, relevant and it can be accessed in a timely manner to meet my needs.	**What an organisation should do to achieve this:** The organisation has effective arrangements in place to systematically categorise, assess, document and improve the quality of its data throughout the data and information life cycle by using a data quality framework that is in line with best practice.

Standard 3.3 Ensure data security	
What a person should expect: I am confident that my information is shared safely and held securely, and that my confidentiality is protected.	**What an organisation should do to achieve this:** The organisation has effective physical and technical security arrangements in place to ensure the confidentiality, integrity and availability of data and information, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.
Standard 3.4 Develop staff capability and capacity for information management	
What a person should expect: I am confident that staff have the skills and knowledge to collect, use and share my information appropriately.	**What an organisation should do to achieve this:** The organisation has effective arrangements in place to routinely identify training needs and deliver required training to enable the development of highly trained and competent staff to manage information in line with relevant legislation, standards, policies, guidance and recommendations.

A description of what an organisation meeting this principle looks like

For organisations involved in delivering health and social care, high-quality information that is aligned with national and international best practice regarding data standards and agreed definitions is crucial for informing clinical decision-making and ultimately, providing safer better care. It is also essential for monitoring disease, planning and managing services, guiding policy-making and public health practice, and conducting research. Good information management practices are key to ensuring high-quality information can be shared safely across organisations and available when needed for the aforementioned purposes. In order to optimise information management practices at all levels, an organisation must be responsive to national and international best practice and emerging technologies in the areas of data standards, data quality and data security. A responsive organisation promotes innovation and maximises the utility of available information, enabling the effective use of information to enhance health and wellbeing.

To promote high-quality, accurate and reliable data collection, an organisation must adopt international standards and common definitions. This includes messaging and document standards, as well as terminology standards, including clinical terminologies and classifications. The adoption of such standards and agreed definitions (in line with the national data dictionary, once available) promotes greater standardisation and comparability of health information, and also enables greater interoperability of systems, and improved data sharing and data linkage. A responsive organisation takes a coordinated and proactive approach to the use and adoption of new and existing national and international standards and definitions, as well as evolving policies, guidance and recommendations which can impact on the sharing and re-use of health information.

The use of standards and definitions is also a key driver of data quality. A responsive organisation adopts a systematic approach to categorising, assessing, improving and maintaining the quality of its data on a continuous basis. Roles and responsibilities with regard to data quality are clearly outlined and communicated across the organisation, with an identified individual overseeing the assessment, monitoring and review of data quality and holding responsibility for the quality of information produced by the organisation. Staff are aware of the importance of data quality and receive adequate training to ensure standards are maintained.

Data security should be a key focus for all organisations, but is a particular area of concern for organisations that process sensitive health and social care data. A responsive organisation applies best practices for the collection, processing, storage, analysis, use, sharing and disposal of data, and continually adapts as new technologies are introduced within this rapidly evolving field. It implements strong technical security measures for data processing, particularly for sharing of personal or sensitive data (for example, enhanced password requirements, two factor authentication, role based access controls, and data encryption) and ensures that physical measures for data storage and processing are secure. Data security is embedded in the culture of a well-run responsive organisation, with data security audits undertaken periodically, identified risks included in the organisation's risk register, and practices continually evolving to mitigate risks relating to data security, including reassurance initiatives for cybersecurity.

A responsive organisation takes a strategic and coordinated approach to ensuring that all staff receive adequate training in order to perform their roles effectively. This includes staff training and continuous professional development in the area of information management, covering key areas such as data rights, data standards, data quality, data security and cyber awareness. This also includes the development of general skills for all staff and specialised skills for staff with specialist information management roles. It is the responsibility of management to ensure that the information management responsibilities of staff working in all areas across all levels of the organisation are identified and clearly communicated. It should be recognised that aspects of information management fall within the roles and responsibilities of all staff working in health and social care organisations. A responsive organisation develops and delivers training plans that reflect this. This enables the development of a highly-trained and competent workforce that can manage information in line with national and international best practice.

Sources of evidence for standards within Principle 3

Through review of documents obtained from the organisation prior to, and during, the site visit, reviewers may:

- Review roles and responsibilities relating to data standards, data quality and data security within the organisation.
- Investigate if the organisation is compliant with relevant data standards, data security standards and data quality requirements.
- Investigate if the organisation has a data dictionary that is aligned with nationally and internationally agreed definitions and updated regularly.
- Review the organisation's approach to data quality and explore whether the organisation has a data quality framework in place.
- Find out if the organisation maintains comprehensive records of its data processing activities and data flows.
- Review the organisation's approach to data security and identify what arrangements are in place to ensure best practices for the collection, storage, use, sharing and disposal of information.
- Investigate the organisation's arrangements for assessing and mitigating physical and technical security risks (including whether it undertakes periodic data security audits).
- Explore the organisation's arrangements for staff training in the area of information management.
- Identify if local and regional policies and procedures are aligned to national policy.
- Support the identification of additional lines of enquiry for the review.

Documents reviewed could include:

- Policies and procedures (covering areas such as acceptable use of ICT resources; data classification and handling; data sharing and information transfer; network security; role based access controls; data storage, archival, retention and destruction; business continuity and disaster recovery)
- Documentation relating to information standards for clinical content, clinical terminologies and classifications; messaging standards for interoperability; data security standards and other relevant standards specific to the organisation's functions
- Data quality strategy documents, assessment tools and reports
- Records of data processing activities

- Data flow maps
- Data dictionaries
- Staff training records and training materials
- Audit records and schedules
- Organisational charts
- Risk registers

HIQA reviewers will communicate with the organisation, and in some situations, observe practice, to:

- Get clarification and further detail regarding any queries that arise through the review of documentation obtained from the organisation.
- Confirm whether there are identifiable individuals with responsibility for standards, data quality and data security within the organisation.
- Explore levels of knowledge and awareness of data standards, data quality (including data quality frameworks), and data security amongst staff working across the organisation.
- Investigate whether staff receive adequate training to manage information in line with relevant legislation, standards, policies, guidance and recommendations.
- Explore whether the physical and technical security arrangements in place are effective for ensuring the confidentiality, integrity and availability of data and information, from the perspectives of staff working within the organisation.
- Find out if staff are familiar with the latest national and international standards, policies, guidance and recommendations for safe and effective collection, use, and sharing of information.

This communication and observation could take the form of:

- Telephone, teleconference, and email contact prior to, and following, the site visits
- Online or in-person meetings, interviews, and focus groups
- System demonstrations and observations of practice.

Indicators of compliance

Standard 3.1: Align with national and international best practice regarding standards and agreed definitions	
Indicators of compliance include:	▪ Evidence of a coordinated approach to the development and implementation of clear policies and procedures to ensure that the most appropriate definitions, standards and classifications are in use, leading to standardised practices across the organisation. ▪ Central oversight and well-established roles relating to standards and definitions, including an identified individual responsible. ▪ Evidence that staff roles and responsibilities with regard to standards and definitions are documented and communicated, with high levels of awareness among staff working across the organisation. ▪ Use of a comprehensive data dictionary that aligns with national policy. ▪ Evidence of engagement with other national and international entities to ensure consistency with regards to standards and definitions. ▪ Evidence of a coordinated approach to reviewing, auditing and updating relevant policies and procedures.
Indicators of substantial compliance include:	▪ Evidence that relevant standards and definitions are in use across the organisation but there is a lack of central oversight and an uncoordinated approach to their implementation, leading to some variation in practices. ▪ At least one identifiable individual with responsibilities relating to standards and definitions; however, the roles are not formalised and some gaps are evident. ▪ Good levels of awareness among staff overall but there is evidence of gaps in staff knowledge relating to some standards and definitions, and their roles and responsibilities relating to these. ▪ A data dictionary is in use but it is not comprehensive or fully aligned with national policy. ▪ Evidence that relevant policies and procedures are reviewed and updated periodically but audited only on an ad hoc basis.

Indicators of partial compliance include:	▪ Policies and procedures with regard to definitions and standards lack detail and are inconsistently implemented across the organisation. ▪ Varying levels of awareness among all staff with regard to standards and definitions, and their roles and responsibilities relating to these. ▪ Evidence that relevant policies and procedures are reviewed and updated on an ad hoc basis but not routinely audited.
Indicators of non-compliance include:	▪ Current policies, procedures and practices are not sufficient to ensure alignment with national and international best practice regarding standards and agreed definitions. ▪ Evidence of few, if any, formal agreed definitions or standards in use. ▪ No individual with responsibility for overseeing the use of standards and definitions across the organisation. ▪ Low levels of awareness among all staff with regard to standards and definitions, and their roles and responsibilities relating to these. ▪ A data dictionary is not in place. ▪ Evidence that relevant policies and procedures are not reviewed, audited or updated regularly.

Standard 3.2: Enhance data quality	
Indicators of compliance include:	▪ Evidence of a coordinated approach to the development and implementation of clear policies and procedures relating to data quality, with a comprehensive data quality framework in place and standardised practices across the organisation. ▪ Use of a data quality framework to routinely assess, document and improve data quality in a standardised way. ▪ Central oversight and well-established roles relating to data quality, including an identified individual responsible. ▪ Evidence that staff roles and responsibilities with regard to data quality are documented and communicated, with high levels of awareness among staff working across the organisation. ▪ Complete records of all data processing activities across the organisation that are maintained and regularly updated. ▪ Evidence of a coordinated approach to reviewing, auditing and updating relevant policies and procedures.
Indicators of substantial compliance include:	▪ Policies, procedures and practices enhance data quality overall, and most elements of a data quality framework are in place, but there is some evidence of gaps in existing policies and procedures leading to some variation in practices. ▪ At least one identifiable individual with responsibilities relating to data quality; however, the roles are not formalised and some gaps are evident. ▪ Good levels of awareness among staff overall but there is evidence of gaps in staff knowledge relating to data quality, and their roles and responsibilities relating to this. ▪ A record of processing activity is available but is not comprehensive and contains some gaps. ▪ Evidence that relevant policies and procedures are reviewed and updated periodically but audited only on an ad hoc basis.
Indicators of partial compliance include:	▪ Policies and procedures with regard to data quality lack detail and there is evidence of only some elements of a data quality framework in place, with no routine monitoring of data quality and inconsistent practices across the organisation.

	▪ Varying levels of awareness among all staff with regard to data quality, and their roles and responsibilities relating to this. ▪ Evidence that relevant policies and procedures are reviewed and updated on an ad hoc basis but not routinely audited.
Indicators of non-compliance include:	▪ Current policies, procedures and practices are not sufficient to enhance data quality. ▪ No evidence of a data quality framework in place or any routine monitoring of data quality. ▪ No individual with assigned responsibility for overseeing data quality across the organisation. ▪ Low levels of awareness among all staff with regard to data quality, and their roles and responsibilities relating to this. ▪ No record of all data processing activities. ▪ Evidence that relevant policies and procedures are not reviewed, audited or updated regularly.

Standard 3.3: Ensure data security	
Indicators of compliance include:	▪ Evidence of a coordinated approach to the development and implementation of clear policies and procedures relating to data security, leading to standardised practices across the organisation. ▪ Central oversight and well-established roles relating to data security, including an identified individual responsible. ▪ Evidence that staff roles and responsibilities with regard to data security and how to respond to a data breach are documented and communicated, with high levels of awareness among staff working across the organisation. ▪ Evidence of strategy and plans for how the organisation can best use existing and emerging technology to improve how it stores and processes information and optimise its data security arrangements. ▪ Physical and technical environments that ensure information is stored and processed securely and prevent unauthorised access. ▪ Evidence of a standardised and coordinated approach to the assessment and management of data security risks. ▪ Evidence of a coordinated approach to reviewing, auditing and updating relevant policies and procedures.
Indicators of substantial compliance include:	▪ Policies, procedures and practices ensure data security overall, but there is evidence of some gaps in how policies and procedures are implemented, leading to some variation in practices. ▪ At least one identifiable individual with responsibilities relating to data security; however, the roles are not formalised and some gaps are evident. ▪ Good levels of awareness among staff overall but there is evidence of gaps in staff knowledge relating to some elements of data security, and their roles and responsibilities relating to this. ▪ Adequate physical and technical environments for information storage and processing overall; however, a lack of strategy and plans for optimising data security arrangements is evident.

	▪ Evidence that relevant policies and procedures are reviewed and updated periodically but audited only on an ad hoc basis.
Indicators of partial compliance include:	▪ Policies relating to data security lack detail and procedures are inconsistently implemented across the organisation. ▪ Varying levels of awareness among all staff with regard data security, and their roles and responsibilities relating to this. ▪ Inconsistent approach to assessing and managing data security risks. ▪ Evidence that relevant policies and procedures are reviewed and updated on an ad hoc basis but not routinely audited.
Indicators of non-compliance include:	▪ Current policies, procedures and practices are not sufficient to ensure data security or to guide the organisation's response to data breaches or other data security risks. ▪ No individual with responsibility for overseeing data security across the organisation. ▪ Low levels of awareness among all staff with regard to data security, and their roles and responsibilities relating to this ▪ A shortage of key physical and technical infrastructure to store and share information securely. ▪ No routine assessment of data security risks. ▪ Evidence that relevant policies and procedures are not reviewed, audited or updated regularly.

Standard 3.4: Develop staff capability and capacity for information management	
Indicators of compliance include:	▪ Evidence of a planned and coordinated approach to staff training on information management across the organisation. ▪ Evidence of annual training needs analyses being conducted and documented. ▪ Arrangements for specific and tailored training for staff with specialist information management roles. ▪ Evidence that levels of participation in staff training are assessed and staff knowledge is audited. ▪ Evidence that all staff have the necessary knowledge and skills relating to information management and are confident in their abilities to perform their roles effectively. ▪ Evidence of a coordinated approach to reviewing, auditing and updating training plans.
Indicators of substantial compliance include:	▪ Evidence that training courses relating to information management are available to all staff, but the overall approach to staff training is somewhat uncoordinated, with some gaps evident in how training needs are assessed and how training plans are developed (for example, some inconsistency evident). ▪ Arrangements for specific and tailored training for some, but not all, staff with specialist roles ▪ Evidence that training plans are reviewed and updated periodically but audited only on an ad hoc basis.
Indicators of partial compliance include:	▪ Evidence of some training needs analyses being conducted and associated training plans completed; however, these are not routine or comprehensive. ▪ Lack of evidence to demonstrate the availability of specific and tailored training for staff with specialist roles. ▪ Evidence that training plans are reviewed and updated on an ad hoc basis but not routinely audited.
Indicators of non-compliance include:	▪ A lack of evidence or records to demonstrate that training needs analyses are conducted. ▪ No evidence of specific and tailored training for staff with specialist roles.

	▪ No evidence to demonstrate that levels of participation in staff training are assessed or that staff knowledge is audited. ▪ Evidence that all staff no not have the necessary knowledge or skills relating to information management to perform their roles effectively. ▪ Evidence that training plans are not reviewed, audited or updated regularly.

Principle 4

Accountability

Responsiveness
A Human Rights-based Approach
Person-centred Care and Support
Safety and Wellbeing
Accountability

Guidance on Principle 4: Accountability

An introduction to the principle

In the context of health and social care information, the principle of accountability relates broadly to having the necessary governance arrangements in place to ensure that an organisation meets its objectives relating to data and information while adhering to all relevant legislation and codes of practice. An accountable organisation operates in a transparent way and takes a strategic approach to planning its services in accordance with the needs of the people about whom it holds information. Achievement of high-quality information management practices is very much dependent on the culture of an organisation in which information management is treated as a high priority.

The standards associated with the principle

Principle 4: Accountability	
Standard 4.1 Develop strong organisational governance, leadership and management	
What a person should expect: I am confident that the organisation is governed and managed in a way that ensures my information is collected, used and shared appropriately.	**What an organisation should do to achieve this:** The organisation has effective strategic governance, leadership and management arrangements in place with clear lines of accountability to ensure that information is collected, used and shared appropriately.
Standard 4.2 Implement strategy for information management	
What a person should expect: I am confident that the organisation has clear plans about how my information will be collected, used and shared to support me and my health and social care needs now and into the future.	**What an organisation should do to achieve this:** The organisation has effective arrangements in place to set clear objectives in relation to the services that it provides and the associated information management and system requirements, and develops a plan for delivering on these objectives.

Standard 4.3 Promote effective performance assurance and risk management	
What a person should expect: I am confident that the organisation assesses its performance and manages risks relating to my information.	**What an organisation should do to achieve this:** The organisation has effective performance assurance and risk management arrangements in place in relation to information management to promote accountability to all stakeholders and to encourage continuous and rigorous self-assessment and improvement.
Standard 4.4 Ensure compliance with relevant legislation and codes of practice	
What a person should expect: I am confident that my information is being collected, used and shared in a way that is aligned with Irish and European law.	**What an organisation should do to achieve this:** The organisation has effective arrangements in place to ensure compliance with relevant Irish and European legislation and codes of practice, and has a process in place for identifying and addressing potential gaps in compliance with existing and forthcoming legislation.

A description of what an organisation meeting this principle looks like

Accountability means having the necessary governance arrangements in place to ensure an organisation's objectives are met while adhering to all relevant legislation and codes of practice. Within the context of information management, an accountable organisation has formalised governance structures in place, including clear lines of accountability and documented roles and responsibilities with regard to all aspects of information management. This includes having an identifiable individual with overall accountability, responsibility and authority for information held by the organisation, as well as other defined roles and responsibilities with regards to key aspects of information management, such as information governance, data quality, data security, data protection, and compliance with relevant legislation and standards. The governance arrangements in place ensure that information is managed effectively and that staff working at all levels of the organisation are clear about their individual and collective roles and responsibilities with regard to information management.

An accountable organisation takes a coordinated and strategic approach to information management. It acknowledges the importance of setting and documenting clear objectives relating to information management and the associated system requirements in order to optimise the accessibility, use and value of information. Such a coordinated and strategic approach is essential to ensuring an organisation delivers on its objectives in the short, medium and long term and remains aligned with all relevant national and international strategies, standards, policies, guidance and recommendations. Achievement of high-quality information management practices requires information management to be reflected in an organisation's overall strategy for information management, and embedded in its oversight and accountability structures. Strategic workforce planning and a proactive approach to identifying workforce gaps and informing human resource strategies is essential to ensure that an organisation has a workforce that is agile and responsive to changes occurring in the health information field.

An accountable organisation demonstrates good practices in transparency and reporting. It publishes an annual report which is accessible to all its stakeholders, including members of the public, and outlines its activities and progress with regard to its objectives throughout the preceding year. Central to accountability is the management of risk and performance in a coordinated way through robust internal control systems and effective performance management practices. A clearly documented and communicated risk management policy and associated processes led and overseen by senior management are essential to ensuring that all risks are assessed and managed appropriately. It is imperative that the identification and management of potential risks relating to information management are treated the same way as other risks and are embedded in an organisation’s risk management policy and associated processes. A schedule of internal and external audits demonstrates that an organisation takes a proactive and coordinated approach to ensuring its policies, procedures and practices are adequate. Finally, carefully selecting and using key performance indicators (KPIs) should provide senior management with assurance that practices are consistently of a high standard.

In an accountable organisation, compliance with applicable legislation and codes of practices is embedded in the organisation's governance and oversight structures. In the rapidly-evolving field of health information, it is essential that organisations have effective arrangements in place to ensure they remain compliant, including having documented roles and responsibilities with regard to reviewing and identifying potential haps in compliance. A proactive approach is essential to ensure that all policies, procedures, and practices remain aligned with both current and future legislation and codes of practice.

Sources of evidence for standards within Principle 4

Through review of documents obtained from the organisation prior to, and during, the site visit, reviewers may:

- Investigate if appropriate oversight and management structures are in place, in line with the size and complexity of the organisation (such as a management team and/or Board that meets regularly), and find out whether information management is embedded within such structures.
- Review roles and responsibilities with regard to information management, and explore whether there are clear lines of accountability for all staff working across the organisation, with roles, responsibilities and reporting arrangements that are clearly documented and communicated.
- Explore whether the organisation takes a strategic approach to information management by setting clear objectives and developing and implementing a plan for delivering on them.
- Explore how the organisation reviews and reports on its performance and demonstrates accountability to all its stakeholders, in particular with regard to its objectives relating to information management.
- Investigate if the organisation is open and transparent with regard to its goals and objectives through the publication of a statement of purpose that is accessible (for example, on the organisation's website) and updated regularly.
- Investigate if appropriate joint governance arrangements are in place with parties with whom the organisation has shared responsibility for deciding the purposes and/or means of how personal information is used (if applicable).
- Find out if formalised agreements are in place with all data providers, data processers and data recipients, as required.
- Examine if the organisation undertakes strategic workforce planning and has plans in place to effectively manage the use of all available resources.
- Explore the organisation's approach to ensuring it is compliant with relevant legislation and codes of practice and find out if it has arrangements in place to prepare for forthcoming legislation.
- Find out if there is there is oversight of the organisation's record of processing activity.
- Identify if local and regional policies and procedures are aligned to national policy.
- Support the identification of additional lines of enquiry for the review.

Documents reviewed could include:

- Organisational charts
- Terms of references for all groups and committees

- Meeting agendas and minutes
- Strategic and business plans
- Annual reports
- Statement of purpose
- Memorandums of understanding and or statements of partnership with other organisations
- Service level agreements, data processing agreements, data sharing agreements and other formalised agreements with data providers, processers and recipients
- Records of processing activity
- Workforce plans
- Documentation of KPIs
- Audit schedules
- Risk registers

HIQA reviewers will communicate with the organisation, and in some situations, observe practice, to:

- Get clarification and further detail regarding any queries that arise through the review of documentation obtained from the organisation.
- Confirm whether there is an identifiable individual with overall accountability, responsibility and authority for information held by the organisation.
- Confirm whether there are identifiable individuals with responsibility for key aspects of information management (for example, data quality, data security, data protection and compliance with legislation).
- Find out if staff are aware of, and familiar with, organisational structures, lines of accountability and other governance arrangements in place at the organisation.
- Explore if there is clarity with regard to roles and responsibilities in situations where joint governance arrangements are in place for particular data processing activities.
- Explore whether quality improvement and the development of learning systems are embedded within the culture of the organisation.

This communication and observation could take the form of:

- Telephone, teleconference, and email contact prior to, and following, the site visits
- Online or in-person meetings, interviews, and focus groups
- System demonstrations and observations of practice.

Indicators of compliance

Standard 4.1: Develop strong organisational governance, leadership and management	
Indicators of compliance include:	▪ Clearly defined governance structures and arrangements which set out lines of authority and accountability and specific roles and responsibilities. ▪ Central oversight of the development, implementation, review, audit and updating of all policies, procedures and practices relating to information management to ensure all information is being managed effectively in accordance with relevant legislation and codes of practice. ▪ Documented terms of reference for, and adequate documentation from the meetings of, key oversight and management groups and other groups or committees that have roles and responsibilities relating to information management. ▪ Central oversight and well-established roles relating to information management, including an identified individual with overall accountability, responsibility, and authority for information held by the organisation. ▪ Evidence that staff roles and responsibilities with regard to information management are documented and communicated, with high levels of awareness among staff working across the organisation. ▪ Evidence of adequate joint governance arrangements with other organisations, as appropriate, and formalised agreements, where required, to support the provision and safe sharing of information. ▪ Evidence of adequate oversight of all data processing activity. ▪ An accessible statement of purpose which sets out the organisation's aims and objectives with regard to information, is aligned with its overall strategy and direction, and is regularly reviewed and updated with input from key stakeholders.

Indicators of substantial compliance include:	▪ Evidence that governance structures and arrangements are mostly adequate, but there are some gaps with regard to overall authority and accountability, and lines of reporting. ▪ Documented terms of reference and documentation from the meetings of most key groups is available; however, this information is lacking or incomplete for some groups and committees or lacks a particular focus on information management. ▪ At least one identifiable individual accountable for information management; however, the roles are not formalised and some gaps are evident. ▪ Good levels of awareness among staff overall but there is evidence of gaps in staff knowledge relating to aspects of information management, and their roles and responsibilities relating to this. ▪ Joint governance arrangements and formalised agreements, where required, are mostly adequate but there is evidence of some gaps with regard to the documented roles and responsibilities of the relevant organisations. ▪ Evidence of adequate oversight of most, but not all, data processing activity. ▪ A statement of purpose is available but is lacking some detail with regard to the organisation’s information management practices.
Indicators of partial compliance include:	▪ Lack of evidence regarding governance structures and arrangements for information management, with a lack of clarity with regard to overall authority and accountability, and lines of reporting. ▪ Varying levels of awareness among all staff with regard to information management, and their roles and responsibilities relating to this. ▪ Joint governance arrangements and formalized agreements with other organisations are in place for some, but not all, data sharing activities.

Indicators of non-compliance include:	▪ Governance structures and arrangements are not effective to ensure the organisation can deliver on its aims and objectives in relation to information management. ▪ No terms of reference or documentation for key groups or committees. ▪ Low levels of awareness among all staff with regard to information management, and their roles and responsibilities relating to this. ▪ No joint governance arrangements with other organisations and no formalised agreements to support the provision and safe sharing of information. ▪ A lack of central oversight of the organisation’s data processing activities. ▪ No documented statement or purpose.

Standard 4.2: Implement strategy for information management	
Indicators of compliance include:	▪ Evidence that the organisation sets clear objectives in relation to the services that it provides and the associated information management and system requirements, and develops a plan for delivering on these objectives. ▪ Evidence of a strategy for building human resource competencies to ensure the availability of a skilled workforce. ▪ Relevant information management skills and competency development are integrated in to training plans for staff working at all levels of the organisation. ▪ Evidence that the organisation is proactive in its approach to ICT and other resources and actively strategises and plans for how it can make best use of existing and emerging technology to improve its practices.
Indicators of substantial compliance include:	▪ Information management is incorporated in to the organisation's strategic plan to some extent, but gaps are evidence for key aspects of information management. ▪ Information management skills and competency development are integrated in to training plans for some, but not all, relevant staff. ▪ An awareness of emerging technology and some initial attempts to strategize and plan for how such technology could be used within the organisation.
Indicators of partial compliance include:	▪ Evidence of some information management strategy at individual team or department level but there is a lack of coordination across the organisation and plans are not available or comprehensive. ▪ Little attempt to strategise and plan for how emerging technology could be used within the organisation.
Indicators of non-compliance include:	▪ No evidence of objectives relating to information management in strategic and business plans. ▪ The lack of a strategy or plan to ensure workforce requirements are met in the short, medium and long term. ▪ A lack of awareness among management of the need for a strategic and coordinated approach to ensure the organisation is managing information in the most appropriate way and making the best use of existing and emerging technologies.

Standard 4.3: Promote effective performance assurance and risk management	
Indicators of compliance include:	▪ Published annual reports which outline the organisation's progress with regard to its business and strategic plans in relation to information management. ▪ Appropriate KPIs are identified and used to measure, report and improve on the organisation's performance. ▪ A schedule of internal and external audits to assess the effectiveness of policies and procedures is available and there is evidence of such audits taking place. ▪ Robust risk management systems are in place, including a risk management policy and a risk register for information management that is regularly reviewed. ▪ A formal complaints procedure to capture positive and negative feedback in relation to information management is available. ▪ Evidence that continuous quality improvement and learning systems are embedded within the culture of the organisation.
Indicators of substantial compliance include:	▪ Annual reports are published but they are not fully comprehensive in relation to progress in relation to information management plans. ▪ The organisation reports on some, but not all, relevant KPIs and there is gaps in evidence regarding how these are used to improve performance. ▪ A schedule of audits is available but not all audits have taken place as scheduled or it is not comprehensive. ▪ A risk management policy is in place but there is some evidence that the risk register is not always reviewed or updated in line with the policy and lacks details regarding information management risks and actions.
Indicators of partial compliance include:	▪ Reports on the organisation's progress are published on an ad hoc basis but lack detail in relation to information management. ▪ Some KPIs are captured but these are not used effectively to improve performance. ▪ No audit schedule available but some audits are performed on an ad hoc basis.

	▪ An inconsistent approach to assessing and managing risks and evidence that information management risks are not adequately captured.
Indicators of non-compliance include:	▪ Reports on the organisation’s progress with regard to its business and strategic plans are not published. ▪ Appropriate KPIs have not been identified. ▪ No schedule of audits or evidence of any taking place. ▪ No routine assessment of risks relating to information management. ▪ No complaints procedure in place.

Standard 4.4: Ensure compliance with relevant legislation and codes of practice	
Indicators of compliance include:	▪ Evidence of a coordinated approach to the development and implementation of clear policies and procedures which ensure that the organisation is compliant with relevant legislation and codes of practice. ▪ Compliance with applicable legislation and codes of practices is reflected in the organisation's overall strategy for information management, and embedded in the organisation's oversight and accountability structures. ▪ Central oversight and well-established roles relating to ensuring compliance with relevant legislation and codes of practice, including an identified individual responsible. ▪ Evidence that staff roles and responsibilities with regard to ensuring compliance with relevant legislation and codes of practice are documented and communicated, with high levels of awareness among staff working across the organisation. ▪ Evidence of a coordinated approach to the assessment and management of risks relating to current or forthcoming legislation. ▪ Evidence of a coordinated approach to reviewing, auditing and updating relevant policies and procedures to assess and ensure continued compliance with relevant legislation and codes of practice.
Indicators of substantial compliance include:	▪ At least one identifiable individual with responsibilities relating to ensuring compliance with relevant legislation and codes of practice; however, the roles are not formalised and some gaps are evident. ▪ Good levels of awareness among staff overall but there is evidence of gaps in staff knowledge relating to some legislation and codes of practice, and their roles and responsibilities relating to these. ▪ Evidence that relevant policies and procedures are reviewed and updated periodically but audited only on an ad hoc basis.
Indicators of partial compliance include:	▪ Evidence of some uncertainty around how the organisation can meet certain obligations with regard to legislation and codes of practice but some steps are being taken to improve levels of understanding across the organisation.

	▪ Varying levels of awareness among all staff with regard to relevant legislation and codes of practice and their roles and responsibilities relating to these. ▪ Inconsistent approach to assessing and managing risks relating to current or forthcoming legislation. ▪ Evidence that relevant policies and procedures are reviewed and updated on an ad hoc basis but not routinely audited.
Indicators of non-compliance include:	▪ Current policies, procedures and practices lack sufficient detail to demonstrate whether the organisation is fully compliant with relevant legislation and codes of practice. ▪ No individual with responsibility for ensuring the organisation is compliant with all relevant legislation and codes of practice. ▪ Low levels of awareness among all staff with regard to relevant legislation and codes of practice, and their roles and responsibilities relating to this. ▪ No routine assessment of risks relating to current or forthcoming legislation. ▪ Evidence that relevant policies and procedures are not reviewed, audited or updated regularly.

References

1. Health Act (2007). Available from: https://www.irishstatutebook.ie/eli/2007/act/23/enacted. Accessed on: 14 December 2023.

2. Child Care Act, (1991). Available from: https://www.irishstatutebook.ie/eli/1991/act/17/enacted/en/html. Accessed on: 14 December 2023.

3. Children Act, (2001). Available from: https://www.irishstatutebook.ie/eli/2001/act/24/enacted/en/html. Accessed on: 14 December 2023.

4. Health Information and Quality Authority. *Guidance on a Human Rights-based Approach in Health and Social Care Services*. Dublin: 2019. Available from: https://www.hiqa.ie/reports-and-publications/guide/guidance-human-rights-based-approach-health-and-social-care-services. Accessed on: 12 December 2022.

5. Transform Health. *Health Data Governance Principles*. 2022. Available from: https://healthdataprinciples.org/. Accessed on: 12 December 2022.

6. Charter of Fundamental Rights of the European Union, (2012). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN. Accessed on: 12 Decemner 2023.

7. General Data Protection Regulation (GDPR), (2018). Available from: https://eur-lex.europa.eu/eli/reg/2016/679/oj. Accessed on: 12 December 2023.

Health Information and Quality Authority
An tÚdarás Um Fhaisnéis agus Cáilíocht Sláinte

Published by the Health Information and Quality Authority.

For further information please contact:

Health Information and Quality Authority
Dublin Regional Office
George's Court
George's Lane
Smithfield
Dublin 7
D07 E98Y

Phone: +353 (0) 1 814 7400
Email: info@hiqa.ie
URL: www.hiqa.ie