Health Information and Quality Authority

An tÚdarás Um Fhaisnéis agus Cáilíocht Sláinte

NATIONAL STANDARDS FOR

Information Management in Health and Social Care

2024

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, in conjunction with the Department of Health and the Health Service Executive (HSE).

Overview of the Health Information and Quality Authority

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

Introduction

Introduction

Data and information are generated in huge volumes everyday across the health and social care system. Information is data that has been processed or analysed to produce something useful.

Good data is the foundation to a high-quality health and social care service. For example, data and information about a person's care and treatment need to be shared between a general practitioner (GP) and hospital in a timely way to ensure they get the best care. High-quality data is also important for other purposes such as planning and managing services, policy-making and research. Although health data 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 data collected is of the highest quality and used to its full potential to promote safer better care, improved outcomes and overall wellbeing.

In recent years, significant legislative developments, including the European General Data Protection Regulation (GDPR), acknowledge the potential high-quality data has on improving services and performance, while recognising the challenges associated with balancing the need to effectively use data with individuals' concerns regarding privacy and confidentiality.[2-4] Further legislative reform, which is currently underway at a national and European level, will promote the re-use of data and reinforce the need for strong governance of health data.[5-8] This will place additional requirements on organisations to manage information appropriately. These standards will help organisations to develop and embed good information management practices, which is fundamental to developing data maturity. The standards will promote the safe and effective use of data, which will allow for enhanced value across the health and social care system.

1.1 Purpose of the national standards

National standards are a set of high-level outcomes that describe how organisations and services can improve practices to achieve safer better care. They are evidence-based and informed by the outcomes of engagement with those who use and provide our health and social care services.

The aim of the *National Standards for Information Management in Health and Social Care* (referred to as national standards for the remainder of the 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.

All relevant standards have a 'use of information' section, highlighting the importance of actively using information as a resource for planning, delivering, monitoring, managing and improving care. The national standards, in conjunction with other health and social care standards developed by HIQA, collectively aim to improve the quality of health information and data, which ultimately contributes to the delivery of safe and reliable health and social care.

It is recognised that the arrangements that each service and organisation put in place to adhere to these standards will vary depending on the type of work they are undertaking and the size and complexity of the system(s), service or organisation; however, the principles, standards and features can all be applied in practice regardless of the size or complexity of the service or organisation or the type of work they undertake.

The primary audience for these standards is organisations within the scope of these standards as outlined in section 1.3. However, given the interconnected nature of health and social care, all services and organisations that collect, use or share health and social care information, including those that fall outside of scope, can use these standards to develop and embed good information management practices. The benefit of a system-wide approach to information management is the potential to improve the quality and use of information across the health and social care system. In addition, these standards also give an outline of what a person should expect from organisations that collect, use and share their information. This is to create a common understanding of what good practice looks like in this area for the person whose data and information is being collected, used and shared.

1.2 HIQA's relevant legislative remit – Health Act 2007

The Health Act 2007 (and amendments)[1] sets out HIQA's relevant legislative remit.* These standards will contribute to safer better care by improving the management of health and social care information:

- Under Section 8(1)(b) of the Health Act 2007 (and amendments),[1] HIQA has a legal mandate to set standards for the safety and quality of health and social care services provided by the HSE, the Child and Family Agency (Tusla), or a service provider in accordance with the Health Acts 1947 to 2007,[1] Child Care Act 1991,[9] and the Children Act 2001.[10]
- Under Section 8(1)(c) of the Health Act 2007 (and amendments),[1] HIQA has a legal mandate to monitor compliance with the standards set under Section 8 (1)(b) of the Act.[1]

* Under the Patient Safety (Notifiable Incidents and Open Disclosure) Act 2023, HIQA's functions to set standards and monitor compliance with standards will be extended to private hospitals and prescribed private health services.

- Under Section 8(1)(i, j, k, l) of the Health Act 2007 (and amendments),[1] HIQA has a legal mandate to evaluate information, provide advice and recommendations about deficiencies identified in respect of the information:
  - (i) to evaluate available information respecting the services and the health and welfare of the population;
  - (j) to provide advice and make recommendations to the Minister and the Executive about deficiencies identified by the Authority in respect of the information referred to in paragraph (i);
  - (k) to set standards as the Authority considers appropriate for the Executive and service providers respecting data and information in their possession in relation to services and the health and welfare of the population;
  - (l) to advise the Minister and the Executive as to the level of compliance by the Executive and service providers with the standards referred to in paragraph (k).

1.3 Scope of the national standards

These standards apply to all organisations and services within HIQA's legislative remit, including services provided by the HSE, Tusla, and relevant service providers with the exception of designated centres* registered and inspected by the Chief Inspector of Social Services in HIQA under Part 8 of the Health Act 2007.[1]

1.3.1 Standards setting and monitoring intent

The national standards have been set under Section 8(1)(b) of the Health Act 2007 (and amendments).[1] HIQA will monitor compliance with the standards as per Section 8(1)(c) of the Health Act 2007 (and amendments).[1]

HIQA will use these standards to review information management practices in national data collections** and eHealth services*** that fall within its remit as outlined above. HIQA will also use the standards to review information management practices at a national level within the HSE and Tusla. The standards may also be used for statutory investigations or to perform thematic inspections in organisations and services that fall within the scope of the standards.

* Designated centres are defined in Section 2 of the Health Act 2007 as residential services for older persons, children and adults with disabilities and special care units for children.

** National data collections are national repositories of routinely collected health and social care data.

*** eHealth services are the technology, people and processes which facilitates the sharing of electronic patient-specific information between health and social care services across organisations and/or care settings.

For the remainder of this document:

The term 'organisation' will be used when referring to service providers, systems and organisations that fall within the scope of these national standards.

The term 'person' will be used to refer to patients, people using services and members of the general public, including children.

1.4 Information management

Information management refers to all processes relating to the collection, storage, management and maintenance of information in all forms, and at any stage of the data and information lifecycle (see infographic on the next page).

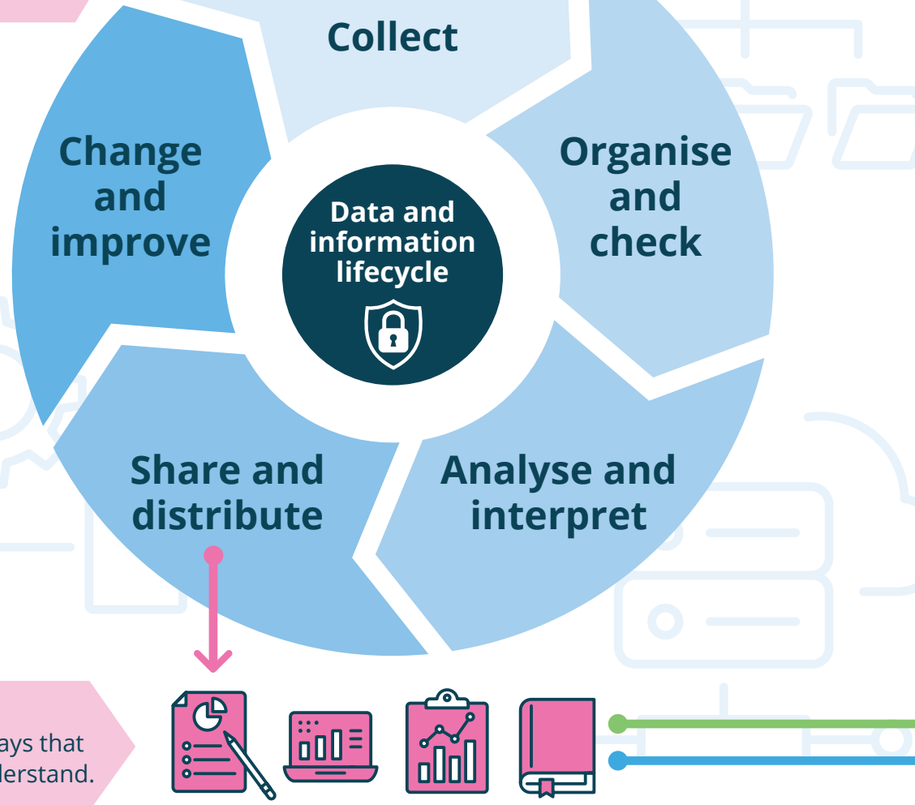
Data and information lifecycle

Health data and information is found in many different sources, such as health records, medical images, prescriptions, laboratory reports, claims and reimbursement data, data from wellness devices, registries and other data collections. When data is analysed or presented to make it more meaningful or useful, it is then often referred to as information. The data and information lifecycle refers to the stages which data goes through to become information, from the point of data collection through to its use.[11]

What is information management?

Before data becomes information, it goes through the following lifecycle:

Data can be numbers, symbols, words, images or graphics that have not yet been organised or analysed.



Information is presented in ways that are easy to understand.

How data and information are used

Primary use of information:

Use of a person's health information to inform their care.

EXAMPLES:

Individuals use their health information to make decisions on their own health and well-being, for example, managing a chronic (ongoing) condition.

Health and social care professionals use health information to decide on what care, support or treatment is best for the person.

Secondary use of information:

Re-using a person's information to help plan and manage health and social care services, inform public health, guide policy-making, and perform research.

EXAMPLES:

Healthcare organisations, such as hospitals, use information to manage services and plan for future needs with the aim of continuously improving quality of care and achieving better value for money.

National data collections use information to inform policy-making, improve public-health and undertake research to compare treatments and services.

Good information management will:

All health and social care professionals are responsible for managing information appropriately.

1 IMPROVE SAFETY AND WELLBEING

by promoting the use of accurate, relevant and timely data to inform good decision-making for both primary and secondary use.

2 BUILD TRUST

by adopting a 'rights-based approach' to information management by effectively engaging with individuals, groups and communities, and using information in a way that respects privacy and promotes equity.

3 PROMOTE BEST PRACTICE

by managing information in line with international best practice by following data security, data quality and data standards requirements.

1.5 Importance of good information management

Good-quality health and social care information that is accurate, relevant and timely is critical to providing safer better care. It is essential to inform good clinical decision-making, monitor disease, plan and mange services at local and national levels, guide policy-making and public health practice, and conduct high-quality research. Inevitable advances in digital health have the potential to improve the quality of care and promote better use of information through safe and effective methods of sharing such as through electronic health records. Considerable time, effort and resources are invested into collecting, using and sharing information and in maintaining the systems that support these processes. It is, therefore, important that everyone working within health and social care services is aware of their responsibilities in terms of managing information appropriately.

As part of a person's journey through the health and social care system, information is collected and shared at different stages using a combination of paper-based and electronic systems. This forms a person's healthcare record and is used to inform their care. Information is shared between staff within and across settings, as appropriate, to support the provision of care (known as the primary use of information). Good information management practices are essential to ensure that information is available when, and where, it is needed, in order to facilitate timely, evidence-based decision-making, to reduce waste and improve service efficiency, and improve safety and quality of care. Good information practices are also essential to ensuring that accurate data is captured in the right format, aligned to data standards and shared in line with legislation to maintain privacy and confidentiality. Information that is collected during the provision of health and social care is also required to compile national data collections which can be used for planning and management of health and social care services, public health, policy-making and research (known as secondary use of information).

The health and social care information landscape is changing based on digital health advances so organisations need to be responsive to the significant changes occurring in the area of health information nationally and internationally, including key legislative changes occurring at both an Irish and European level.[5,6] In particular, the establishment of a European Health Data Space (EHDS) will promote easier exchange and better re-use of health information.[6] This requires organisations to manage information in line with international best practice, and adhere to requirements in the areas of data security, data quality and data interoperability standards. All organisations and services, therefore, need to take a coordinated and strategic approach to information management to ensure data is collected, used and shared effectively with the appropriate safeguards in place to protect privacy and confidentiality. Plans should include how they will engage with key stakeholders, including people using services, the public and professionals, and incorporate their perspectives into how information is managed.

Good information management is imperative to ensuring that levels of trust in the systems used to process such information are nurtured, and that organisations ensure they are meeting their objectives in terms of the effective use of information, while respecting the privacy of people about whom the information relates to. It is, therefore, important that everyone working in organisations that collect, use and share health and social care information receive the appropriate training to understand how information is used for different purposes and to keep up to date with rapidly evolving information management practices.

1.6 Principles underpinning the national standards

Good information management practices are guided by the principles underpinning the national standards:

- **Human rights-based approach:** 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. Transparency on how information is collected, used and shared is essential. The use of confidential information needs to be justified, required and limited to what is necessary; access should be based on a strict need-to-know basis; and those with access should be aware of their responsibilities and obligations. Individuals, groups and communities with diverse needs and requirements should be involved in decision-making regarding how their information is managed, and their views should be incorporated in relevant policies and procedures. This should guide equitable information management practices in which the health value created by the use of data must fairly benefit individuals, groups and communities.[12]

- **Safety and wellbeing:** An organisation needs accurate, relevant and timely information to deliver and monitor safe and high-quality care for every person. Through effective engagement with key stakeholders, organisations need to design, develop and maintain data and systems to ensure a person and professionals involved in their care have access to accurate information and to enable safe sharing of data for primary and secondary uses. It is important that a person can easily access information, including their own records, to promote enhanced safety and wellbeing. Information should also be used to continuously drive improvements to service provision and outcomes. Emerging and evolving technologies have to be safe, secure and reliable, including artificial intelligence (AI) and machine learning, and should be used to enhance safety and wellbeing.

- **Responsiveness:** Information should be managed in line with international best practice regarding relevant health information standards. Organisations also need a systematic approach to assessing, improving and maintaining the quality of its data on a continuous basis. A strategic and proactive approach to security is essential to ensure that a person's information is being managed in a safe and secure way to build trust and confidence. An organisation needs to have arrangements in place to ensure it can adapt and respond to evolving health information standards and other requirements in terms of emerging technologies. A responsive organisation also has highly trained and competent staff to manage information in line with national and international best practice.

- **Accountability:** An organisation should have appropriate governance arrangements in place to ensure a strategic approach to information management is adopted. This will ensure that performance and risks are managed, and that objectives relating to data and information are met, while adhering to all relevant legislation. Information should be managed in a way that is cost-effective and ensures it is fit for purpose when needed.

1.7 Structure of the national standards

The national standards consist of three sections: principles, standards and features. These elements are intended to work together, and collectively, they describe best practice in terms of information management for organisations that collect, use and share health and social care information.

Principles:

HIQA's principles-based framework is used for the development of all national standards. Standards are presented under the four principles: a human rights-based approach, safety and wellbeing, responsiveness and accountability.

Standards:

A set of high-level outcomes that describe how services can achieve safer better care by improving the management of health and social care information. Each standard statement is comprised of two elements:

Standard	
What a person should expect:	**What an organisation must do to achieve this:**
A statement written from the perspective of a person from which the data was collected regarding what they would expect from the organisation.	A statement setting out the arrangements that an organisation processing health and social care data must have in place to achieve the desired outcomes.

Features:

Each standard is accompanied by a list of features which, when taken together, show how an organisation can demonstrate that it is meeting the standard. The list of features under each standard statement is not intended to be exhaustive, and the organisation may meet the requirements of the standards in other ways.

1.8 Summary of the national standard statements

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.

Principle 2: Safety and wellbeing

Standard 2.1: Optimise the accessibility, use and value of information

What a person should expect:	What an organisation should do to achieve this:
I am confident that my information is used, in line with legislation and innovation, to continuously drive improvements in care, safety and wellbeing.	The organisation has effective arrangements in place to use data and information as a resource in the planning, delivery 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:	What an organisation should do to achieve this:
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.	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.

Principle 3: Responsiveness

Standard 3.1 Align with best practice regarding data standards and agreed definitions	
What a person should expect:	**What an organisation should do to achieve this:**
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.	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:	**What an organisation should do to achieve this:**
I am confident that my information is accurate, relevant and it can be accessed in a timely manner to meet my needs.	The organisation has effective arrangements in place to systematically categorise, assess, document and improve the quality of its data throughout the data and information lifecycle by using a data quality framework that is in line with best practice.
Standard 3.3 Ensure data security	
What a person should expect:	**What an organisation should do to achieve this:**
I am confident that my information is shared safely and held securely, and that my confidentiality is protected.	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:	**What an organisation should do to achieve this:**
I am confident that staff have the skills and knowledge to collect, use and share my information appropriately.	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.

Principle 4: Accountability

Standard 4.1 Develop strong organisational governance, leadership and management

What a person should expect:	What an organisation should do to achieve this:
I am confident that the organisation is governed and managed in a way that ensures my information is collected, used and shared appropriately.	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:	What an organisation should do to achieve this:
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.	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.

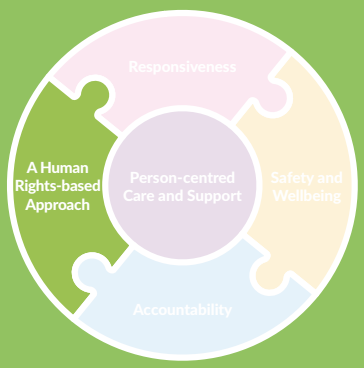
Standard 4.3 Promote effective performance assurance and risk management

What a person should expect:	What an organisation should do to achieve this:
I am confident that the organisation assesses its performance and manages risks relating to my information.	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:	What an organisation should do to achieve this:
I am confident that my information is being collected, used and shared in a way that is aligned with Irish and European law.	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.

Principle 1



A human rights-based approach

Principle 1:
A human rights-based approach

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. Data protection is a fundamental right as set out in Article 8 of the European Charter of Fundamental Rights.[13] The specific rights of a person in respect of their personal data are set out in GDPR.[2] Broader rights, in a health and social care context, include the right to autonomy and to make informed choices, the right to be treated with dignity and respect and in an equal and non-discriminatory manner, and the right to safety. Organisations have to balance rights in relation to their data against other values, fundamental rights, human rights, and legitimate public or vital interests.[14] This can only be achieved by evaluating information management practices to identify and mitigate any potential harm which may occur at an individual, group or community level.[12] Examples of individual or collective risk include: loss of privacy, risk to personal safety, risk of insufficient or incorrect care, risks to public health or risk to unequal benefit from data contribution. Information management practices must reduce any potential risks.

A human rights-based approach is underpinned by a legal framework and human rights treaties which Ireland and other states have agreed to uphold. FREDA is an internationally recognised framework through which human rights can be considered under the following five principles: Fairness, Respect, Equality, Dignity and Autonomy.[14] A human rights-based approach means that the organisation views the people about whom it holds information, including professionals, as equal partners in planning, developing and monitoring its information management policies and processes. Organisations should 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.

Organisations can promote a human rights-based approach in the context of health and social care information by following the standards outlined in this section.

Standard 1.1
Uphold people's rights relating to information

Standard 1.1	
What a person should expect:	**What an organisation should do to achieve this:**
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.	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.

Features of an organisation meeting this standard may include:

1.1.1 Ensuring clarity on what people's rights are in relation to their data and the choices they have about their data. 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* (see feature 1.2.2).

1.1.2 Documenting and communicating a clear process for obtaining informed consent for the use of health data for specific purposes and for facilitating people to change their consent preferences.

1.1.3 Ensuring effective arrangements are in place to align practices with relevant legal frameworks and human rights treaties which establish data rights.** This should include, but is not limited to:

- Ensuring relevant policies and procedures are aligned with legal frameworks and human rights treaties.
- Documenting and communicating roles and responsibilities of staff within the organisation to ensure rights relating to data are upheld (see feature 4.1.2).

* There are limitations and conditions contained within the data protection rights set out under the GDPR. For example, certain data protection rights only apply in certain circumstances, such as right to erasure, which only applies where the personal data is no longer required for the purpose it was originally collected.

** For example, legal sources of human rights and equality obligations are found in: the Irish Constitution 1937; the European Convention on Human Rights Act 2003; the Charter of Fundamental Rights of the European Union 2000; the Equal Status Acts 2000-2015; the Irish Human Rights and Equality Commission Act 2014; the ratification of international treaties that have evolved from the Universal Declaration of Human Rights, including the United Nations Convention on the Rights of Persons with Disabilities (UNCRPD) 2006; and the introduction of the Assisted Decision-Making (Capacity) Act 2015.

1.1.4 Ensuring effective arrangements are in place to promote an inclusive, sensitive and equitable approach to information management for individuals, groups and communities with diverse needs by considering data collection methodologies and processes, intended uses and accessibility to information.*

* Information is collected, used and shared in such a way that respects diversity, including life experience, age, gender, culture, language, disability, beliefs and identity. This process may include consideration for equity stratifiers. These are variables chosen to reflect a perceived inequality which help to compare data on specific groups of people.

Standard 1.2
Protect privacy and confidentiality

Standard 1.2	
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.

Features of an organisation meeting this standard may include:

1.2.1 Identifying an individual whose role includes providing education, advice, guidance and support to the organisation and staff in the area of data protection, such as a Data Protection Officer (DPO) or someone with an assigned information governance role (see feature 4.1.2).

1.2.2 Publishing and regularly reviewing a privacy statement or notice which clearly outlines what information is collected, how it is used and shared, and a point of contact to facilitate feedback and review.

1.2.3 Undertaking Data Protection Impact Assessments (DPIAs)* to identify and mitigate any data protection-related risks arising from new and ongoing projects. The organisation may consider publishing a summary of findings and/or actions arising from the DPIA.

1.2.4 Ensuring effective arrangements are in place to check that the collection, use and sharing of personal information is justified, required, limited to what is necessary and that access to personal confidential data is on a strict need-to-know basis (see features 3.3.3 and 3.3.5).

1.2.5 Developing, implementing, reviewing and auditing policies and procedures to protect privacy. These may include, but are not limited to, the following areas:

- Privacy and confidentiality
- Data access and request, including requests regarding personal data
- Document and records management
- Data breach management**
- Data security (see standard 3.3).

* Guidance on Privacy (Data Protection) Impact Assessment is available on HIQA's website: www.hiqa.ie.

** A documented and implemented process for a suspected or actual personal data security breach to ensure all appropriate actions are taken to safeguard the data and the privacy of individuals and to prevent similar breaches in the future.

Principle 2

Safety and wellbeing

Principle 2:
Safety and wellbeing

Access to timely, accurate and relevant information is the foundation of high-quality and safe service provision, effective planning and management, and overall better outcomes and wellbeing. Appropriate information management can drive a culture of safety in an organisation by providing information in the right form, in the right place, and at the right time, with the appropriate safeguards in place. In certain emergency situations, access to up-to-date and accurate information saves lives. In addition, information collected as part of routine care should be used to continuously drive improvements in safety and wellbeing. The implementation of the EHDS regulation and the establishment of a health data access body will further support and enhance the effective re-use of data for secondary purposes enabling appropriate data linkage and de-identification for specified purposes. The benefits of effectively using information to promote safety and wellbeing include: improving a person's outcome and experience; identifying and reducing waste, and improving efficiency of services; generating knowledge through audit and research, and continuously applying learnings; identifying and monitoring epidemiological trends; and enhancing education, training and performance of staff.

Access to data and the sharing of information across services and organisations, **for primary and secondary use of information,** is not only critical for a person's safety, it also results in better evidence-based decision-making at every level and ultimately leads to better outcomes. Information drawn from high-quality data can also empower a person to make informed choices about their care, and to maintain and improve their overall health and wellbeing. Services and organisations should strive to provide a person with access to their own health information.

Organisations that use information to promote safety and wellbeing should:

- strategically aim to optimise, through emerging and evolving technologies,[15] the accessibility, use and value of information for primary and secondary purposes to improve safety and wellbeing. This includes at a personal level to inform choices; at service provision level to inform clinical decision-making, and to plan and manage services; and at local, regional and national level to inform policy-making, manage public health, enhance resource allocation and promote research.
- undertake effective stakeholder engagement to promote safety and wellbeing. This involves facilitating and encouraging active participation of all relevant stakeholders, including people using services, the general public and professionals. In this context, meaningful stakeholder engagement ensures that people about whom the information relates, as well as other key users of the information, 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.

Organisations can promote safety and wellbeing in the context of health and social care information by following the standards outlined in this section.

Standard 2.1
Optimise the accessibility, use and value of information

Standard 2.1	
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, delivery 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.

Features of an organisation meeting this standard may include:

2.1.1 Providing access to high-quality information, in line with legislation, to promote effective and safe use of data in a timely manner to improve safety and wellbeing.* This includes, but is not limited to:

- personal access to health and social care records to help decide on best treatment or care and to promote changing behaviour based on public health advice or new research
- information-sharing within and between services to support clinical decision-making and enhance patient safety
- information on the quality and safety of its services, using internationally recognised quality indicators such as key performance indicators (KPIs), which are relevant to all stakeholders including the public
- information for policy-making and management of services including the planning, monitoring, delivery, improvement, auditing and evaluation of such services
- information to identify or prevent threats to public health
- information to drive effective innovation through research and quality improvement.

2.1.2 Promoting effective use of resources and infrastructure (including software, information and communication technology (ICT) equipment, cloud services) to enable safe access to data to support safety and wellbeing, and to support learning health systems in line with emerging and evolving technologies. These should align with national digital health policy and strategies, as well as relevant broader sector developments. This may include, but is not limited to:

* Following the FAIR (Findability, Accessibility, Interoperability and Reusability) Guiding Principles.

- National digital health initiatives
- Ireland's Open Data portal
- Web-based tools for accessing and analysing data, and for business intelligence
- Secure processing environments for the safe linkage, analysis and management of personal data
- AI and machine learning.

2.1.3 Uniquely identifying individuals,* providers**, locations and assets to enhance safety, and to promote effective use of information for both primary and secondary purposes including through the use of data linkage, in line with national policy, standards and best practice.

2.1.4 Establishing data sharing rules and guidelines,*** including defining multiple levels of data access**** in association with policies and procedures (see feature 1.2.5).

2.1.5 Assessing and managing risks associated with information sharing using the Five Safes Framework, when appropriate, including: safe data; safe projects; safe people; safe settings; and safe outputs.*****

2.1.6 Ensuring business continuity and continuity of care, and having disaster recovery plans in place to facilitate timely response to an event which may impact on accessibility or use of information.

2.1.7 Routinely monitoring the accessibility, use and value of information to identify areas for improvement.

* A method to uniquely and safely identify each person that has used, is using or may use a health or social care service in Ireland.

** Up to date information on health sites, locations, health care providers and services

*** Rules should outline limitations on data access, identifying which stakeholders will have access to various levels of data, including de-identified or aggregated data.

**** Considering data sharing required for individual care delivery, among public agencies, between government systems, private sector and with international stakeholders, if required.

***** The Five Safes Framework is used for helping make decisions about the effective use of data which is confidential or sensitive.[16]

Standard 2.2
Undertake effective stakeholder engagement

Standard 2.2	
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.

Features of an organisation meeting this standard may include:

2.2.1 Performing a stakeholder analysis to identify key stakeholders, including people using services, members of the public, marginalised groups,* professionals and other users of the data.

2.2.2 Engaging with key stakeholders to understand the benefits and risks associated with sharing data and empowering people to make informed choices about their health data and information.

2.2.3 Working with key stakeholders to develop and inform relevant policies and procedures for the organisation with respect to information management.

2.2.4 Ensuring all stakeholders are involved in the co-design of new health information initiatives or systems to inform developments regarding accessibility to information and the associated system design and requirements, and to act as partners in the evaluation of any such initiatives or systems.

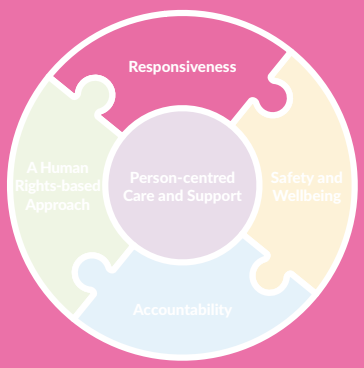
2.2.5 Identifying priorities, expectations and diverse needs of stakeholders to determine and design outputs, such as reports, as well as the most appropriate and meaningful indicators of person's safety and quality of care outcomes.

2.2.6 Establishing learning communities to inform and evolve practices regarding how routinely-collected data can be used to achieve continuous and collective improvements in safety and wellbeing.

* Some considerations include: life experience, age, gender, culture, beliefs, identity, disability, language and literacy levels.

Principle 3

Responsiveness



Principle 3: Responsiveness

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, responsiveness means ensuring the organisation is aligned with best practices nationally and internationally, drives innovation through the adoption of emerging technologies, and ensuring the use of good quality data, with appropriate safeguards in place to ensure maximum benefit is achieved from information. Responsive organisations and services:

- are ready to adapt and ensure compliance with relevant health information standards, policies, guidance and recommendations which may impact on the sharing and re-use of health and social care information
- adopt a systematic approach to categorising, assessing, improving and maintaining the quality of its data on a continuous basis and ensure that lessons learned are routinely incorporated into changes in practices, policies and procedures
- have appropriate arrangements and safeguards in place to ensure that a person's data is managed in a safe and secure way. This requires a strategic and proactive approach to data and information security within a rapidly evolving field
- perform an annual training-needs analysis and deliver required training to enable the development of a highly-trained and competent workforce that can manage information in line with national and international best practice.

Organisations can promote responsiveness in the context of health and social care information by following the standards outlined in this section.

Standard 3.1
Align with best practice regarding standards and agreed definitions

Standard 3.1	
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.

Features of an organisation meeting this standard may include:

3.1.1 Identifying an individual whose role includes the oversight of systems to ensure compliance with relevant standards, policies, guidance and recommendations, as well as identification of future requirements relating to forthcoming standards and agreed definitions.

3.1.2 Ensuring effective arrangements are in place to ensure compliance with relevant standards that are formally issued by standards development organisations, regulatory bodies or other relevant organisations, where appropriate, in the areas of:

- Information standards for clinical content
- Information standards for clinical terminologies and classifications
- Messaging standards for interoperability
- Data security standards (see standard 3.3)
- Other relevant standards specific to organisations functions.*

3.1.3 Developing and implementing a data dictionary to ensure consistency and comparability of data. This should be published, updated in a timely manner and should comply with nationally and internationally agreed definitions where they exist.**

* Organisations should conduct a gap analysis to identify and implement relevant standards appropriate to their function.

** This should align with the HSE National Health and Social Care Data Dictionary, once available.

Standard 3.2
Enhance data quality

Standard 3.2	
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 assess, document and improve the quality of its data throughout the data and information lifecycle by using a data quality framework that is in line with best practice.

Features of an organisation meeting this standard may include:

3.2.1 Identifying an individual whose role includes the oversight of the systematic assessment, monitoring and reviewing of data quality (see feature 4.1.2).

3.2.2 Using a data quality framework* to outline the approaches to assessing, documenting and improving data quality in a standardised way. This should include the following components:

- A data quality strategy – setting out the activities that the organisation needs to undertake in order to strengthen their approach to the collection, handling, use and dissemination of data and information
- A data quality assessment tool – comprising of a set of criteria to comprehensively assess the quality of data sources
- Data quality reports – detailing findings of internal or external data quality assessments, reporting on KPIs or metrics, outlining progress of quality improvements, as well as producing data quality statements
- A data quality improvement cycle – encompassing the processes and methodologies applied by the organisation as part of their data quality improvement initiatives.

3.2.3 Comprehensively mapping data flows in order to detail all data entering and leaving the organisation. This should be informed by a record of all data processing activities and used to help with the segregation of data quality activities (see feature 4.1.5).

* Guidance on a data quality framework and associated modules are available on HIQA's website: www.hiqa.ie

Standard 3.3
Ensure data security

Standard 3.3	
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.

Features of an organisation meeting this standard may include:

3.3.1 Identifying an individual whose role includes oversight and implementation of data security infrastructure, policies and procedures (see feature 4.1.2).

3.3.2 Developing adequate physical and technical environments to ensure information is stored and processed in a secure and suitable way that prevents unauthorised access and ensures it is accessible and retrievable for as long as required.

3.3.3 Implementing role-based access controls to ensure access rights and permissions are based on the information required to fulfil one's role and responsibilities.

3.3.4 Ensuring effective arrangements are in place for data protection and data security structures, including:

- Clearly documenting roles and responsibilities of all staff within the organisation to ensure accountability and increase awareness of data security, including cyber security
- Undertaking security risk assessments which should be linked to the organisation's risk appetite and risk register. The risk assessment cycle should identify, analyse and evaluate physical and technical security risks and determine practical steps to minimise the risks*
- Developing a schedule of internal and external audits and vulnerability assessments to systematically identify opportunities to improve data security practices and cyber security

* Safeguards may include using unique identifiers in place of a person's name; placing limits on how long data may be stored in line with the organisation's retention policy; adding enhanced security measures for personally-identifiable or otherwise sensitive data, such as enhanced password requirements, two-factor authentication, security keys, and data encryption; reassurance initiatives on cybersecurity; ongoing vulnerability assessment including penetration testing; and safe storage guidelines for confidential data.

- Proactively monitoring and implementing measures to improve data security controls on a regular basis, determined by the organisation
- Regularly reporting results to senior management to demonstrate the extent to which the organisation is assured of its data security arrangements.

3.3.5 Ensuring effective arrangements are in place to develop, implement, review and audit policies and procedures for investigating and responding to potential security risks and to promote adequate data protection. This may include, but is not limited to the following areas:

- Acceptable use of ICT resources
- Data classification and handling
- Information transfer
- Network security, including role-based access controls
- Data storage, archival, retention and destruction
- Business continuity and disaster recovery plans (see feature 2.1.6)
- Cloud computing (if applicable).

Standard 3.4
Develop staff capability and capacity for information management

Standard 3.4	
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.

Features of an organisation meeting this standard may include:

3.4.1 Conducting an annual training needs analysis and delivering associated training plans to ensure continuous professional development for staff in the area of information management.

3.4.2 Providing ongoing training and education to all staff to assist them in meeting their information management responsibilities. At a minimum, all staff (and contractors) should receive training to ensure:

- people's rights relating to their data are upheld
- obligations relating to data protection are clear
- appropriate use of data standards and agreed definitions
- continuous improvements to data quality
- best practice in relation to data security and cyber awareness
- compliance with relevant legislation and codes of practice.

3.4.3 Facilitating ongoing professional development for staff with specialist information management roles to align with evolving information management trends. Specialised training should be tailored to specific roles, enabling staff with key information management responsibilities to keep up to date with current and future information management practices.

3.4.4 Performing regular review of training plans and auditing of knowledge to ensure staff are aware of, and adhere to, relevant policies and procedures.

Principle 4

Accountability

Principle 4: Accountability

Strong information management is the foundation of a well-governed and managed organisation. Accountability means that organisations have the necessary governance arrangements in place to ensure its objectives are met in relation to data and information while adhering to all relevant legislation. An accountable organisation also ensures it operates in a transparent way and that its services and objectives are planned in accordance with the needs of the people about whom it holds information and follows a person-centred approach to optimise its information management practices.

Robust accountability through strong governance, leadership and management is essential for organisations to develop and embed good information management practices. Effective arrangements for information management are necessary to ensure that processes, policies and procedures are developed, implemented and adhered to in respect of information management. 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. This acknowledges that data is central to all strategies, as well as being necessary to drive innovation, and to deliver safe and integrated care across services. As governance and data maturity are inextricably linked, there is a critical need for organisations to improve information management practices to promote accountability and to deliver optimal value and public benefit.[17] An accountable organisation that has effective governance, leadership and management ensures the following are in place:

- Formalised governance arrangements, including clear lines of accountability at individual staff member, team and organisational levels so that everyone is aware of their roles and responsibilities with regards to information management. This includes roles and responsibilities with regards to information governance, data quality and data security.
- Business and strategic plans which have a specific focus on how information management is continuously improved. These strategic plans, whether outlined in the organisation's overall strategy or in a specific information management strategy, should be aligned with broader national and international health information strategies. Business plans are essential to translate strategic plans into realistic work targets and to provide a basis for monitoring progress to ensure that key outcomes are achieved within specified timelines.
- Robust performance assessment which involves selecting and using KPIs to evaluate and manage the quality and effectiveness of the organisation's performance, undertaking regular audits to assess practice and having a comprehensive risk management framework in place across all levels of the organisation to help identify, manage and control information-related risks.

- Adequate knowledge, skills and competencies within the workforce to ensure that information is managed effectively at all levels and to ensure compliance with relevant Irish and European legislation. It is imperative that organisations have the appropriate expertise to review current and future requirements in the area of information management, and to lead on the development of relevant policies and procedures to ensure they remain compliant.

Organisations can promote accountability in the context of health and social care information by following the standards outlined in the following section.

Standard 4.1
Develop strong organisational governance, leadership and management

Standard 4.1	
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.

Features of an organisation meeting this standard may include:

4.1.1 Developing a well-defined governance and organisational structure to ensure that the organisation's current and anticipated needs are met in order to support effective decision-making and to plan, design, manage and deliver services. This involves embedding information management within the wider organisational structures including at the levels of:

- an oversight committee or board* – to develop the strategic direction for information management and to ensure that the relevant mission and values are upheld
- a management team, or equivalent – to hold responsibility for planning and delivering its objectives in relation to information management
- other governance groups as appropriate – to fulfil relevant functions such as an information governance committee.

4.1.2 Ensuring clear lines of accountability for all staff members to promote a shared understanding of roles and responsibilities in relation to information management. This includes keeping an updated organisational chart with clear lines of accountability for all staff and outlining specific information management roles and responsibilities such as:

- Identifying an individual with overall accountability, responsibility and authority for information held by the organisation
- Identifying individuals with specific information management roles, for example: information governance, data quality, data security, data protection, and compliance with relevant legislation and standards
- Documenting and communicating relevant responsibilities for information management in the job specifications for all staff.**

* If relevant to the size and complexity of the service or organisation.

** A RACI (Responsible, Accountable, Consulted and Informed) matrix can be used to identify and communicate roles and responsibilities with the organisation.

4.1.3 In situations where joint governance arrangements or joint data controllers* are required, clearly outlining the roles and responsibilities of each organisation to provide assurances that all information is handled legally and securely. This could take the form of a memorandum of understanding or a statement of partnership, where appropriate.

4.1.4 Formalising agreements between data providers, data processers and data recipients, where appropriate, to provide clarity around roles and responsibilities, and to support the provision and safe sharing of quality data. These could take the form of:

- service-level agreements
- data processing agreements
- data sharing agreements.

4.1.5 Ensuring oversight of all datasets or systems by identifying, documenting and controlling activity. This includes keeping an updated record of processing activity and assigning a data controller with responsibility for each to oversee their management. A record of processing activity should include details of what data is being processed and for what purposes, the locations of where processing occurs, and the names of the data controllers and processors (see feature 3.2.3).

4.1.6 Publishing a statement of purpose in an accessible format. This should be aligned with the overall strategy and direction of the organisation, clearly and accurately outlining what the organisation sets out to achieve in terms of information management. This should be reviewed regularly with input from relevant stakeholders (see standard 2.2).

* Joint data controllers are two or more parties that together decide the purposes and/or means of how personal data is used.

Standard 4.2
Implement strategy for information management

Standard 4.2	
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.

Features of an organisation meeting this standard may include:

4.2.1 Developing a plan that sets clear direction for delivering on its objectives in relation to information management in the short, medium and long term. Depending on the size and complexity of the organisation and the services it offers, objectives relating to information management should take account of:

- overall strategic and business plans
- current and future needs in relation technological and infrastructure requirements
- optimising the accessibility, use and value of information through effective sharing* and dissemination**
- effective engagement with key stakeholders to inform developments regarding accessibility of information and the associated system design and requirements (see feature 2.2.1)
- evolving data security requirements to identify and respond to new or potential security risks
- national and international strategies, standards, policies, guidance and recommendations relating to health information.

4.2.2 Undertaking strategic workforce planning that takes account of the size, complexity and objectives of the organisation, the assessed needs of all stakeholders and the best available evidence.

4.2.3 Ensuring effective management of the use of resources, including human, physical and ICT resources, to ensure continued sustainability.

* Data sharing - making data available to another agency, organisation or person under agreed conditions.

** Data dissemination - making non-identifiable or aggregated data publicly available with few or no restrictions on who may access the data and what they may do with it, for example in annual reports.

Standard 4.3
Promote effective performance assurance and risk management

Standard 4.3	
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.

Features of an organisation meeting this standard may include:

4.3.1 Publishing an annual report on progress against business and strategic plans for key stakeholders, including people about whom it holds information.

4.3.2 Promoting a culture of continuous quality improvement and developing learning systems. This includes responding to, and learning from, audits, significant events, reviews, evaluations, feedback and complaints.

4.3.3 Undertaking regular review of its performance relating to information management and clearly identifying roles and responsibilities of committees including reporting arrangements to senior management. This should include, but is not limited to:

- Developing and assessing progress against annual business plans
- Measuring and reporting on organisation's performance using KPIs*
- Undertaking a schedule of internal and external audits to assess compliance with relevant legislation and policies and procedures
- Ensuring robust risk management to assure that all information management-related risks are assessed and managed appropriately, including regular review of the risk management policy and risk register
- Capturing positive and negative feedback on information management, including a formal complaints procedure.

* This relates to the identification, monitoring and reviewing of appropriate KPIs for organisational performance. KPIs for specific areas such as data quality and data security are addressed within standards 3.2 and 3.3.

Standard 4.4
Ensure compliance with relevant legislation and codes of practice

Standard 4.4	
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.

Features of an organisation meeting this standard may include:

4.4.1 Identifying an individual whose role includes the review and identification of gaps in compliance with existing legislation, identification of future requirements with regard to forthcoming legislation and the performance of key roles that are outlined in relevant legislation, including that of a DPO (see feature 4.1.2).

4.4.2 Ensuring effective arrangements are in place to assess compliance with relevant existing Irish and European legislation and codes of practice. This includes:

- having clear oversight and relevant documentation regarding developing, implementing, reviewing and auditing of policies and procedures in a timely way in line with relevant legislation.
- regularly reviewing risks related to current or forthcoming legislation including data protection-related risks and learning from suspected or actual breach of legislation.

References

1. Health Act 2007. Available from: https://www.irishstatutebook.ie/eli/2007/act/23/enacted/en/html. Accessed on: 15/06/23.
2. General Data Protection Regulation 2018. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02016R0679-20160504. Accessed on: 15/06/23.
3. Data Protection Act 2018. Available from: https://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html. Accessed on: 15/06/23.
4. Data Protection Act 2018 (Section 36(2)) (Health Research) (Amendment) Regulations 2021. Available from: https://www.irishstatutebook.ie/eli/2021/si/18/made/en/print. Accessed on: 15/06/23.
5. Health Information Bill - General Scheme 2023. Available from: https://www.gov.ie/en/publication/6f6a6-health-information-bill-2023/. Accessed on: 15/06/23.
6. Proposal for a regulation - The European Health Data Space 2022. Available from: https://health.ec.europa.eu/publications/proposal-regulation-european-health-data-space_en. Accessed on: 15/06/23.
7. Data Governance Act - regulation (eu) 2022/868 of the european parliament and of the council 2022. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0868. Accessed on: 15/06/23.
8. Proposal for a regulation of the european parliament and of the council on harmonised rules on fair access to and use of data (Data Act) 2022. Available from: https://data.consilium.europa.eu/doc/document/ST-6596-2022-INIT/en/pdf. Accessed on: 15/06/23.
9. Child Care Act 1991. Available from: https://www.irishstatutebook.ie/eli/1991/act/17/enacted/en/html. Accessed on: 15/06/23.
10. Children Act 2001. Available from: https://www.irishstatutebook.ie/eli/2001/act/24/enacted/en/html. Accessed on: 15/06/23.
11. Canadian Institute for Health Information. *CIHI's Information Quality Framework*. Ottawa: 2017. Available from: https://www.cihi.ca/sites/default/files/document/iqf-summary-july-26-2017-en-web_0.pdf. Accessed on: 06/12/21.
12. Health Data Governance Principles 2022. Available from: https://healthdataprinciples.org/. Accessed on: 15/06/23.
13. European Union. *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: 08/06/22.

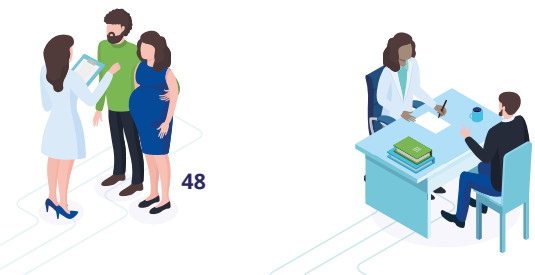
14. Health Information and Quality Authority. Guidance on a Human Rights-based Approach in Health and Social Care Services 2019. Available from: https://www.hiqa.ie/sites/default/files/2019-11/Human-Rights-Based-Approach-Guide.PDF. Accessed on: 15/06/23.

15. Trade and Employment Department of Enterprise. AI - Here for Good: National Artificial Intelligence Strategy for Ireland 2021. Available from: https://www.gov.ie/en/publication/91f74-national-ai-strategy/. Accessed on: 15/06/23.

16. Felix Ritchie. *The 'Five Safes': a framework for planning, designing and evaluating data access solutions*. 2017.

17. United Nations. Data Strategy of the Secretary-General for Action by Everyone, Everywhere 2020. Available from: https://www.un.org/en/content/datastrategy/images/pdf/UN_SG_Data-Strategy.pdf. Accessed on: 15/06/23.

18. Health Information and Quality Authority. *Evidence synthesis of international evidence on governance structures and information management arrangements in place for national health and social care data collections*. Dublin: 2022. Available from: https://www.hiqa.ie/reports-and-publications/health-information/evidence-synthesis-international-evidence-governance. Accessed on: 03/07/23.



Key terms used in this report

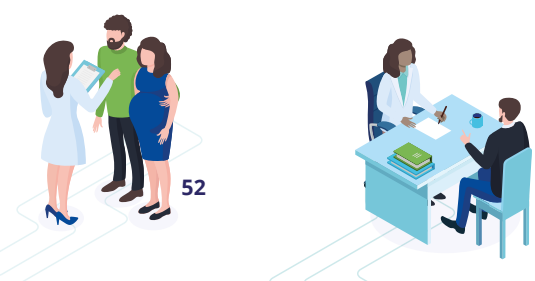
Aggregate data	Data that has been summarised and or categorised to a level that ensures the identities of individuals or organisations cannot be determined by a reasonably foreseeable method.
Artificial intelligence	Refers to machine-based systems, with varying levels of autonomy that can, for a given set of human-defined objectives, make predictions, recommendations or decisions using data.
Clinical classifications	Provide a framework for the recording of data and information in a uniform, relevant and consistent way, by using a 'common language'. An example is the International Statistical Classification of Diseases and Related Health Problems 10th Revision (ICD-10).
Clinical terminologies	A structured collection of descriptive terms for use in clinical practice, used by clinicians to describe the assessment of and care given to a person during a consultation. An example is the Systematised Nomenclature Of Medicine-Clinical Terms (SNOMED-CT).
Co-design	A process for developing products, initiatives, and strategies directly with stakeholders by actively involving them in the design process.
Consent	Any freely given specific, informed and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to them.
Data	The building blocks for information. Described as numbers, symbols, words, images and graphics that have been validated but not yet organised or analysed.
Data and information lifecycle	Refers to the stages which data goes through to become information, from the point of data collection through to its use.
Data controller	A person, company, or other body which decides the purposes and methods of processing personal data.
Data dictionary	A document that outlines the 'rules' by which all the data in a particular system or collection need to abide by, including the names, definitions and attributes of all data elements to be collected; it standardises definitions and ensures consistency of data.

Data linkage	A method of bringing information from different sources together about the same person or entity to create a new, richer dataset.
Data processor	A person, company, or other body which processes personal data on behalf of a data controller.
Data processing agreement	A legally binding document to be entered into between the controller and the processor which regulates the scope and purpose of processing, as well as the relationship between the controller and the processor.
Data protection impact assessment (DPIA)	A process designed to identify risks arising out of the processing of personal data and to minimise these risks as far and as early as possible. DPIAs are important tools for negating risk, and for demonstrating compliance with the GDPR.
Data protection officer	A leadership role required in organisations; responsible for overseeing an organisation's data protection strategy and its implementation to ensure compliance with GDPR requirements.
Data quality framework	An organisations approaches to systematically assessing, documenting and improving data quality and includes data quality policies and procedures; key performance indicators and metrics; audits; and improvement initiatives.
Data quality statement	A statement published to highlight the dimensions of data quality, including strengths and weaknesses, so that potential data users can make informed judgments about fitness for use.
De-identified data or information	Data or information that has been processed so that there is a reduced likelihood of a person being reasonably identified, although re-identification may be possible through deliberate techniques, such as linkage with other data sources.
Equitable approach to information management	Equity in information management includes representation in data of all individuals, groups and communities, regardless of social or economic characteristics, as well as equitable access to data-generated health value. Equity should be addressed in policies, processes but also through public engagement, education and meaningful participation of all groups in relevant decision-making about health data systems.[12]
Equity stratifiers variables	Variables selected to reflect perceived inequalities in the population that is the subject of the data collection. The most frequently used equity stratifiers in healthcare are: place of residence; race (or ethnicity); occupation; gender (or sex); religion; education; socioeconomic status; social capital.

Key performance indicators (KPIs)	Specific and measurable elements of practice that are designed to assess key aspects of structures, processes and outcomes.
Information	Data that has been processed or analysed to produce something useful.
Information governance	The arrangements that are in place to manage information to support an organisation's immediate and future regulatory, legal, risk, environmental and operational requirements relating to information.
Information management	The processes relating to the collection, storage, management, and maintenance of information in all forms.
Lawful processing	In order to process personal data, an organisation must have a lawful basis to do so. Under Article 6 of the GDPR, the lawful grounds for processing personal data are: individual consent; a contract; a legal obligation; vital interests of a person; public interest; legitimate interests of the organisation.
Learning Health System	Internal data and experience are systematically integrated with external evidence, and that knowledge is put into practice.
Open data portal	Publication of Irish Public Sector data in open, free and reusable formats.
Personal data or information	Data or information about a living person, where that person either is identified or could be identified.
Primary use of information	Collection, use and sharing of health information for the purpose of providing health and social care.
Privacy notice or statement	A public document from an organisation that explains how that organisation processes personal data and how it applies data protection principles.
Secondary use of information	Collection, use and sharing of health information for reasons beyond direct care such as planning and management of health services, policy-making, public health and research.
Unique identifier	A unique, non-transferable lifetime number assigned to a person. Its purpose is to identify the individual and to allow the "attaching" of other information (such as name, address and contact details) to them.

Glossary of abbreviations

AI	Artificial intelligence
DPO	Data Protection Officer
DPIA	Data Protection Impact Assessment
EHDS	European Health Data Space
GDPR	General Data Protection Regulation
GP	General practitioner
HIQA	Health Information and Quality Authority
HSE	Health Service Executive
ICT	Information and Communication Technology
KPI	Key performance indicator



Appendix 1
How the national standards were developed

The national standards were developed in line with HIQA's standards development process. The standard statements and features were informed by an evidence synthesis, consultation with an advisory group as well as a public consultation and targeted consultation.

Stage 1: Evidence synthesis – An evidence synthesis of international evidence on governance structures and information management arrangements in place for national health and social care data collections was conducted in 2022 which includes an 'as-is' analysis of the current situation in Ireland. This paper was used to inform the national standards and ensures that they are evidence-based and fit for purpose in an Irish context.[18]

Stage 2: Advisory group – At the beginning of the standards development process, an advisory group was established to provide expert advice (see **Table 1** for list of members). The Advisory Group is made up of a diverse range of interested and informed parties. At each stage of the process, members of the Advisory Group had an opportunity to input to the development of the standards. This included informing the scope of the project, providing feedback on the draft standards prior to public consultation, submitting a response to the public consultation, and providing further feedback on the standards following the public consultation process.

Stage 3: Public consultation and targeted consultation – An eight-week public consultation ran from 24 October 2022 to 19 December 2022 to gather feedback on the content and structure of the draft standards. The draft standards document was made publicly available to download on www.hiqa.ie and a consultation feedback form was developed to assist people to make submissions. Submissions could be made using an online survey tool, emailed to a dedicated email address, or posted to HIQA.

At the start of the public consultation, the Project Team notified members of the Advisory Group that the public consultation had commenced and asked that they inform the organisations and groups they represent of this. The Project Team also contacted relevant health and social care professionals, policy-makers, advocacy groups and interested stakeholders by email to inform them of the process and request that they share information about the public consultation and encourage their colleagues and members of the public connected to their services to participate in the process. In order to reach as wide a range of stakeholders as possible, the public consultation was advertised in HIQA's newsletter and on its website. In addition, a press release about the public consultation was issued, and the consultation was advertised periodically via HIQA's social media channels, including Twitter, Facebook, LinkedIn and Instagram.

During the public consultation process, the project team held five focus groups with 47 individuals to discuss the draft standards. The focus groups comprised representatives of the health and social care workforce (n = 23 across two focus groups), HIQA inspectors (n = 8) and representatives of national data collections (n = 8) and private hospitals (n=8). For each focus group, a copy of the draft standards, the link to the consultation webpage, and a briefing document on the aims and process of the focus group were sent to participants. All focus groups were conducted online.

Meetings (n=5) were also held with targeted stakeholders to discuss specific details of the draft standards based on their particular expertise.

Stage 4: Publication of standards – All responses from the public and targeted consultations, including consultation feedback forms, and focus group and interview notes, were reviewed and used to inform the development of the standards. Subsequently, the standards were presented to the Advisory Group for its consideration in April 2023. Following analysis and review of the additional feedback, the standards were completed and sent for approval to the HIQA Executive Management Team, before approval by the HIQA Standards Information Research and Technology (SIRT) committee, a sub-committee of its Board, and then the HIQA Board. After the HIQA Board approved the standards, they were submitted to the Minister for Health for approval, and published on the HIQA website.

Table 1. Advisory group membership

Name	Organisation - Title
Azul O'Flaherty	Department of Health - *Assistant Principal, Health Information Policy Unit*
Clíona O'Donovan	National Office for Clinical Audit - *Quality Assurance and Operations Manager*
Colin White	HSE National Patient Representative Panel - *Member*
David Stratton	Primary Care Reimbursement Service, HSE - *Business Manager, PCRS*
Deirdre Murray	National Cancer Registry Ireland - *Director*
Derek McCormack	Operational Performance and Integration, HSE - *General Manager, Acute Business Information Unit*
Eve Robinson	Health Protection Surveillance Centre, HSE - *Specialist in Public Health Medicine*
Fiona Boland	Royal College of Surgeons in Ireland - *Lecturer, Data Science Centre, School of Population Health*
Fiona Kearney	Tusla - *Records Management Lead*
Jacqui Curley	Healthcare Pricing Office - *Head of HIPE and NPRS*

Name	Organisation - Title
Jennifer Martin	Quality and Safety Directorate, HSE - *Clinical Lead, Quality and Patient Safety Intelligence*
Johnny Sweeney	Irish College of General Practitioners - *Project Manager, National General Practice IT Project*
Ken Moore	Central Statistics Office - *Senior Statistician, Quality Management Support and Assurance Division*
Laura Heavey	National Screening Service, HSE - *Specialist in Public Health Medicine*
Mark Conroy	Tusla - *ICT Data and Analytics Manager*
Margaret Hynds O'Flanaghan**	CORU - *Head of Recognition*
Maurice Farnan**	HSE - *Interim National Director Community Operations*
Michael Courtney	Department of Health - *Statistician*
Michael Power	HSE National Patient and Service User Forum - *Member*
Pawel Stepala**	Mental Health Commission - *Head of Regulatory Practice and Standards*
Sandra Ryan	Office of the Chief Information Officer, HSE - *Technical Standards Lead*
Sarah Craig	Health Research Board - *Head of National Health Information Systems*
Selina Ryan	Health Informatics Society of Ireland (HISI) - *Nurse Lead for Informatics, St James's Hospital*
Simon Woodworth	University College Cork - *Director, Health Information Systems Research Centre*
Theresa Barry	HSE - *Clinical Terminology Architecture Lead*
Tibbs Pereira	Patients for Patients Safety Ireland - *Member*
Tom Foley**	HSE - *Consultant Psychiatrist*
Tracy Kelleher	National Cancer Registry Ireland - *Data Integration Supervisor*
Trevor Duffy	Royal College of Physicians in Ireland - *Director of Healthcare Leadership*
Trish King**	HSE - *General Manager, Scheduled Care, Acute Operations*

** Additional members invited to join the advisory group to broaden representation after the scope of standards was expanded.

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

© Health Information and Quality Authority 2024