Health Information and Quality Authority

An tÚdarás Um Fhaisnéis agus Cáilíocht Sláinte

DRAFT NATIONAL STANDARDS FOR INFORMATION MANAGEMENT IN HEALTH AND SOCIAL CARE

FOR CONSULTATION

OCTOBER 2022

About the Health Information and Quality Authority

The Health Information and Quality Authority (HIQA) is an independent statutory authority 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.

HIQA's mandate to date extends across a wide range of public, private and voluntary sector services. 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 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 health services and children's social services, and investigating as necessary serious concerns about the health and welfare of people who use these 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 services, in conjunction with the Department of Health and the Health Service Executive (HSE).

Overview of the health information function of HIQA

Health is information-intensive, generating huge volumes of data every day. Health and social care workers spend a significant amount of their time handling information, collecting it, looking for it and storing it. It is, therefore, very important that information is managed in the most effective way possible in order to ensure a high-quality safe service.

Safe, reliable healthcare depends on access to, and the use of, information that is accurate, valid, reliable, timely, relevant, legible and complete. For example, when giving a patient a drug, a nurse needs to be sure that they are administering the appropriate dose of the correct drug to the right patient and that the patient is not allergic to it. Similarly, lack of up-to-date information can lead to the unnecessary duplication of tests — if critical diagnostic results are missing or overlooked, tests have to be repeated unnecessarily and, at best, appropriate treatment is delayed or at worst not given. In addition, health information has an important role to play in healthcare planning decisions — where to locate a new service, whether or not to introduce a new national screening programme and decisions on best value for money in health and social care provision.

Under Section (8)(1)(k) of the Health Act 2007,[(1)] the Health Information and Quality Authority (HIQA) has responsibility for setting standards for all aspects of health information and monitoring compliance with those standards. In addition, under Section 8(1)(j), HIQA is charged with evaluating the quality of the information available on health and social care and making recommendations in relation to improving its quality and filling in gaps where information is needed but is not currently available.

Information and communications technology (ICT) has a critical role to play in ensuring that information to promote quality and safety in health and social care settings is available when and where it is required. For example, it can generate alerts in the event that a patient is prescribed medication to which they are allergic. Further to this, it can support a much faster, more reliable and safer referral system between the patient's general practitioner and hospitals.

Although there are a number of examples of good practice, the current ICT infrastructure in health and social care services in Ireland is highly fragmented with major gaps and silos of information. This results in individuals being asked to provide the same information on multiple occasions.

In Ireland, information can be lost, documentation is poor, and there is an overreliance on memory. Equally, those responsible for planning our services experience great difficulty in bringing together information in order to make informed decisions. Variability in practice leads to variability in outcomes and cost

of care. Furthermore, we are all being encouraged to take more responsibility for our own health and wellbeing, yet it can be very difficult to find consistent, understandable and trustworthy information on which to base our decisions.

As a result of these deficiencies, there is a clear and pressing need to develop a coherent and integrated approach to health information, based on standards and international best practice. A robust health information environment will allow all stakeholders — patients and service users, health professionals, policy-makers and the general public — to make choices or decisions based on the best available information. This is a fundamental requirement for a highly reliable healthcare system.

Through its health information function, HIQA is addressing these issues and working to ensure that high-quality health and social care information is available to support the delivery, planning and monitoring of services.

Table of Contents

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.
Anonymisation	The processing of data or information with the aim of irreversibly preventing the identification of the individual to whom it relates.
Anonymised data or information	Data or information that cannot be traced back to an identified person.
Classification systems	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 patients during a consultation. An example is the Systematised Nomenclature Of Medicine-Clinical Terms (SNOMED-CT).
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 linkage	A method of bringing information from different sources together about the same person or entity to create a new, richer dataset.
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 quality framework	A document which outlines an organisation's approaches to systematically assess, document and improve data quality and includes data quality policies and procedures; key

	performance indicators and metrics; audits; and improvement initiatives.
Data quality statement	A statement prepared to accompany all published outputs from an organisation which highlights 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 an individual being reasonably identified, although re-identification may be possible through deliberate techniques, such as linkage with other data sources.
Equity stratifiers	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.
Personal data or information	Data or information about a living person, where that person either is identified or could be identified.
Pseudonymisation	The processing of personal data or information in such a way that it can no longer be attributed to a specific individual without the use of additional information, provided that — (a) such additional information is kept separately from the data, and (b) is subject to technical and

	organisational measures to ensure that the data is not attributed to an identified or identifiable individual.
Unique identifier	A unique, non-transferable lifetime number assigned to an individual. Its purpose is to identify the individual as one and the same person and to allow the "attaching" of other information (such as name, address, contact details) to them.

Key concepts under the General Data Protection Regulation (GDPR)

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 controller	A person, company, or other body which decides the purposes and methods of processing personal data.
Data processor	A person, company, or other body which processes personal data on behalf of a data controller.
Data processing contract	A legally binding contract governing the processing of personal data when a data processor is engaged to process personal data on the instruction of a data controller.
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.
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.
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.
Special categories of data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; genetic data; biometric data processed to uniquely identify a person; data concerning health; and data concerning a person's sex life or sexual orientation. These categories of data are subject to additional protection under the GDPR, and their processing is generally prohibited, except for where specific requirements are met (such as having explicit consent), as set out in detail in Article 9 of the GDPR.

Glossary of abbreviations

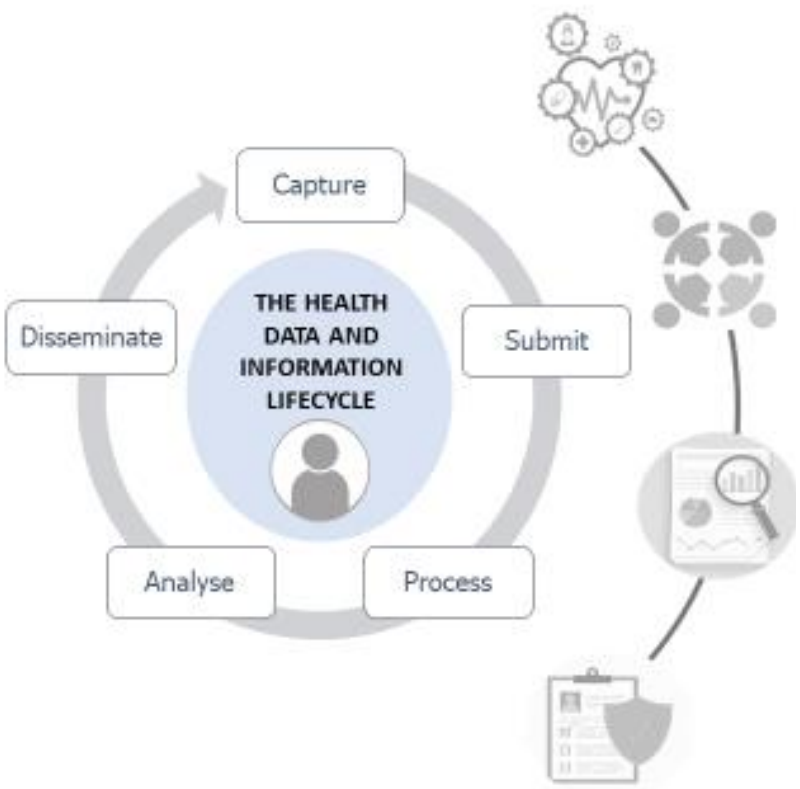
CIDR	Computerised Infectious Disease Reporting
DPIA	Data Protection Impact Assessment
EHR	Electronic Health Record
EU	European Union
GDPR	General Data Protection Regulation
HIPE	Hospital In-Patient Enquiry
HIQA	Health Information and Quality Authority
HRCDC	Health Research Consent Declaration Committee
HSE	Health Service Executive
ICT	Information and Communication Technology
IHI	Individual Health Identifier
KPI	Key Performance Indicator
NIMIS	National Integrated Medical Imaging System
SNOMED-CT	Systematised Nomenclature Of Medicine-Clinical Terms

Introduction

The *Draft National Standards for Information Management in Health and Social Care* were developed to promote a more strategic approach to information management across the health and social care system. Improvements to the quality of health and social care information will contribute to the delivery of safe and reliable care.

Data and information

Data* is generated in huge volumes everyday across the health and social care system. It is a valuable resource and there are significant costs associated with its collection, use and storage; therefore, it is imperative that data collected is of the highest quality and used to its full potential.(2)



INFORMING CARE
As part of an individual's journey through the health and social care system, data is collected and shared at different stages using a combination of paper-based and electronic systems. This forms a patient's record and is used to inform their care.

OTHER PURPOSES
This data can also be used for other purposes, such as for managing and improving local services, and compiling the major national data collections that are used to monitor diseases, manage services, inform policy making, conduct research, and plan for future health and social care needs.

INFORMATION MANAGEMENT
Good information management practices are important at every stage to ensure data is accurate and of good quality and that it is available to inform decisions when required and can be used to its full potential. The stages in the collection, use and sharing of data is often referred to as the data and information lifecycle.

Figure 1 The health data and information lifecycle in the context of an individual's journey through the health and social care system

* Examples of sources of health data include health records, medical images, prescriptions, laboratory reports, claims and reimbursement data, patient reported outcomes, data from wellness devices.

When data is processed, interpreted, organised, analysed, structured, or presented so as it 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 dissemination of information.(3)

If collected, used and shared effectively with appropriate safeguards in place, good data and information can support effective decision-making and problem-solving; inform research and policy; enable an organisation to measure activity, performance and success; result in services that are more aligned with stakeholders' needs; and support better policies and strategies.(4)

For the most part, the term 'information' will be used throughout this standards document; however, the term 'data' will be used in some instances where it is more appropriate.

The collection, use and sharing of health and social care information in Ireland

Across health and social care services in Ireland, information is collected from individuals, recorded in paper-based and electronic records, and shared between staff within and across settings, as appropriate, to support the provision of care. This includes, but is not limited to, the recording of demographic information in patient management systems used in hospital and general practice settings so that a person can be correctly identified by care providers; the sending of referral forms from general practice settings to hospitals to ensure timely access to appropriate services; maintaining up-to-date waiting lists to ensure equitable access to treatment; and the use of various electronic and paper-based systems for managing patients' medical, laboratory and imaging records. Some of these processes are supported operationally by a number of eHealth systems, such as the national integrated medical imaging system (NIMIS) and the national electronic referrals programme. The use of information in this way across health and social care services, sometimes referred to as the **primary use of information**, is essential for informed clinical decision-making and for the provision of safe and effective care.

Information that is collected during the provision of direct care to individuals is subsequently used to compile the major repositories of data that are used to monitor diseases, manage services, inform policy-making, conduct research, and plan for future health and social care needs. The use and sharing of health information for these purposes, sometimes referred to as the **secondary use of information**, is essential for the effective functioning and management of health and social care services. Examples include large administrative data collections such as the Hospital In-Patient Enquiry (HIPE) scheme, the Computerised Infectious Disease Reporting (CIDR) system, and the National Incident Management System (NIMS), which are used for monitoring and reporting on hospital inpatient activity, infectious diseases, and healthcare incidents, respectively. It also includes other repositories of data that are collated and reported on nationally in order to monitor and report on the performance of health and social care services, such as emergency department activity data, national waiting list data, community healthcare data, and ambulance service data.

Examples of the different types of systems that exist at service provider-level (for example, in general practice settings, hospitals, community healthcare settings, and social care services) and at a national-level within the HSE and Tusla to which these standards could be applied are provided in **Table 1**.[†]

[†] Please note: Table 1 provides a number of examples but is not intended to be a comprehensive list of all systems to which these standards could be applied.

Table 1 Examples of systems currently in place at service provider-level and national-level to which these standards could be applied

Type of system	Description	Examples	
		Service provider-level	**National-level within the HSE and Tusla**
Administrative systems and eHealth systems[‡]	Systems used to capture and store routinely-collected patient data and electronic systems used in the delivery of care to service users.	▪ Hospital and general practice patient administration or management systems (e.g. iPMS) ▪ Hospital electronic health records (EHRs)	▪ HIPE scheme ▪ Primary Care Reimbursement Service ▪ National Childcare Information System ▪ National electronic referral programme ▪ National Integrated Medical Imaging System (NIMIS ▪ National Electronic prescribing (ePrescribing)
Registries and Clinical Audits	Organised systems of data collection that use observational methods to collect uniform data (clinical and other) on an ongoing basis on a population defined by a particular disease, condition or exposure.[(5)]	▪ Patient registries ▪ Hospital-level maternity and perinatal clinical audit data	▪ National cancer screening registers, for example, BreastCheck ▪ National Perinatal Reporting System

The term 'service providers and managing organisations' refers to all health and social care organisations, including service providers, national data collections, and national divisions or units of the HSE and Tusla, whose remit involves the collection, use and sharing of health and social care information.

For the remainder of this document, the term 'organisation' will be used when referring to such service providers and managing organisations that fall within the scope of these draft national standards.

[‡] eHealth systems are defined in the eHealth Strategy for Ireland (2013) as: 'patient-centric' and involve the use of modern information systems and technologies to integrate and coordinate the delivery of healthcare to ensure improved patient outcomes, greater efficiencies of delivery, higher levels of transparency and improved ease of access.

What is information management?

Information management refers to all of the processes relating to the collection, storage, management, and maintenance of information in all forms at any stage of the data and information cycle.

Good information management closely aligns with effective information governance, of which the key pillars are:

- ensuring the collection of high-quality data;
- maintaining the privacy and confidentiality of individuals, in line with legislation;
- holding data and information securely; and
- promoting and facilitating effective use of the data use to ensure the maximum benefit for the population.(6)

Based on international best practice, five key overarching objectives relating to information management in health and social care have been identified which are based on maximising health benefits for individuals and for the populations as a whole, specifically:

1. Information is used to deliver and monitor safe and high quality care for everyone.
2. Information should be of the highest quality and where appropriate, collected as close as possible to the point of care.
3. Information should be collected once and used many times to deliver better outcomes for the public.
4. Information should be 'fit for purpose' and cost-effective.
5. Information management should be underpinned by a rights-based approach.

Importance of information management

An individual's health information informs all aspects of their care including assessment, diagnosis, treatment options and prognosis. The Sláintecare Report and subsequent plans and strategies have acknowledged the importance of high quality data and information to drive improvements in the future of healthcare in Ireland.[7,8] The effective management of information across the health and social care system is essential to to achieving the Sláintecare vision of providing the right care, in the right place, at the right time, and ensuring a high-quality safe service for all.

At a service provider level, good information management practices are essential to ensuring 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 patient safety and quality of care. Good information practices at this level are also essential to ensuring that accurate data is captured in the right format, aligned to data standards, and adequate for compiling the major national repositories of data.

At a national level, good information management practices are essential to ensure that such repositories of data are of high quality as the data is used for many important purposes such as to monitor diseases, manage services, inform policy-making, conduct research, and plan for future health and social care needs. Good information management practices are also essential to provide assurances to individuals that their data will be stored safely and managed appropriately to protect their privacy and confidentiality. Overall, for organisations such as the HSE and Tusla, considerable time, effort and resources are invested into collecting, using and sharing information and in maintaining the systems that support these processes at all levels.

The need for good quality and timely information was evident when a rapid response was required of the health and social care system during the COVID-19 pandemic. A concerted effort was placed on optimising the use of new and existing health information systems, which resulted in a number of positive initiatives including: the creation of the COVID Care Tracker to facilitate contact tracing; the development of an online portal to allow laboratories to report daily testing activity; the creation of a reporting dashboard to provide regular reports on the incidence of COVID-19; and the use of the individual health identifier (IHI) in the COVID-19 Vaccine Information System. However, it is clear that a more long-term strategic approach to improving how health information is managed is essential.

Other ongoing developments taking place at a European level are further emphasising the need for good information management practices, including the planned establishment of a European Health Data Space. The primary aim of this

initiative is to promote easier exchange and better re-use of existing information. This requires organisations to manage information in line with international best practice, as well as adhering to data security, data quality and data interoperability standards.

As health and social care information is likely to play an increasing role in the delivery and management of, and planning for, health and social care services, it is imperative that attention is given to ensuring that levels of trust in the systems used to process such information are maintained, and that organisations ensure they are meeting their objectives, while respecting the privacy of individuals about whom the information relates to. To achieve this, organisations need to take a co-ordinated and strategic approach to information management, including plans for how they will engage with key stakeholders and incorporate their perspectives into all policies and processes. They need to implement a sequence of robust arrangements, including formalising governance structures and clearly outlining information governance responsibilities throughout the organisation. Organisations must take a strategic and systematic approach to data quality and data security, and should be ready to adapt 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.

The HSE and Tusla have statutory responsibilities to manage and deliver health and social care services to the population of Ireland. In order to ensure the delivery of safe and effective care, staff working at all levels of both organisations need to be assured of the quality of information – including its accuracy and timeliness – upon which key decisions are being made. A standardised approach to information management practices across all levels of the health and social care system is essential to providing such assurances.

Relevant legislative developments

In recent years, there have been a number of significant legislative changes that have had implications for organisations that process health and social care information. At a European-level, the enactment of the General Data Protection Regulation (GDPR) in 2018 introduced higher standards of data protection for individuals and imposed increased obligations on organisations.[9] It set out six legal bases under which personal data concerning health can be processed. In Ireland, in order to ensure consistency with the GDPR, the Data Protection Act was amended in 2018.[10] As part of this amendment, the Health Research Regulations 2018 were enacted, which make 'explicit consent' the lawful basis for using a patient's personal data in research, unless a consent exemption is sought, and subsequently the Health Research Consent Declaration Committee (HRCDC) was established as an independent statutory body to assess applications for consent declarations.[11,12]

There are likely to be further implications for organisations that process health and social care information over the coming years with the significant national legislative reform currently underway, including the advancement and development of the proposed Health Information Bill and the Patient Safety (Notifiable Patient Safety Incidents) Bill. Data protection is also central to forthcoming European legislative changes which will have a significant impact on the use and sharing of health and social care information across Europe. This includes the planned enactment of the Data Act which sets out rules on fair access to, and use of, data in order to make more data available for use across the European Union (EU), and the Data Governance Act which is focussed on the re-use of data that is protected by the public sector, including health data. The forthcoming legislation emphasises the need to ensure that health information is protected by measures to safeguard the fundamental rights and interests of individuals which is key to the ongoing efforts to progress the European Health Data Space.

Purpose of the draft national standards

The aim of the *Draft National Standards for Information Management in Health and Social Care* (referred to at times in this report as the draft national standards) is to provide a roadmap to improve the quality of national health and social care information, which will ultimately contribute to the delivery of safe and reliable care.

The primary objective of the standards is:

- to improve information management practices across all levels of the health and social care system by promoting a coordinated and strategic approach to information management at all stages of the data and information lifecycle.

It is important to view information management in the context of an interdependent system as it relates to activity at all levels of the health and social care system. Information management is important at every stage of the data and information lifecycle as poor information management in one part of the lifecycle or system may ultimately affect the integrity of the data and information from that point forward. Therefore, a whole-system approach is required to drive real improvements in the quality of health and social care information in Ireland.

Scope of the draft national standards

In order to provide safe and effective care to individuals, and to provide assurances with regards to the quality of information being used to inform the management of health and social care services, effective information management practices must be in place at all levels of the health and social care system. These draft national standards should facilitate a more coordinated and strategic approach to information management within the HSE and Tusla. To improve information management across

the entire system, they need to be used by all services and organisations that collect, use or share health and social care information at any stage of the data and information lifecycle. See Table 1 for examples of the types of systems to which these standards could be applied at both a service provider level and a national level within the HSE and Tusla.

HIQA's Regulatory Remit

As outlined in the Health Act 2007 (and Amendments), HIQA has a legal mandate to set standards for health information for the HSE, Tusla, and associated service providers and to monitor compliance with them, as set out in Section 8 of the Act.[1] HIQA also has a legal mandate to set standards for the safety and quality of health and social care services provided by the HSE, Tusla, or a service provider in accordance with the Health Acts 1947 to 2007,[1] Child Care Act 1991,[13] and the Children Act 2001,[14] and to monitor compliance with them.

Given the interconnected nature of health and social care, a system-wide approach is necessary to ensure that all organisations put in place arrangements to manage information appropriately. Therefore, all services and organisations that collect, use or share health and social care information, including those that fall outside of HIQA's legislative remit, are strongly encouraged to apply these standards as a roadmap to improve the quality and use of information across the entire system. It is recognised that the arrangements that each service and organisation puts in place will vary depending on the type of work they are undertaking and the size and complexity of that 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 Draft National Standards for Health and Social Care will replace the following sets of HIQA standards that currently apply to information management practices in the HSE and Tusla:

- Information management standards for national health and social care data collections (2017)
- Information Governance and Management Standards for the Health Identifiers Operator in Ireland (2015).

Interaction with other national standards

These standards 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 *Draft National Standards for Information Management in Health and Social Care,* in conjunction with other health and social care standards, 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.

How the draft national standards were developed

The *Draft National Standards for Information Management in Health and Social Care* represent a revision and expansion in scope of HIQA's *Information Management Standards for National Health and Social Care Data Collections* which were first published in 2017. This revision was undertaken in order to reflect changes in the health information landscape since then, including legislative and policy changes, and to broaden the scope of the standards to include all organisations that collect, use or share health and social care information at any stage of the data and information lifecycle.

The draft national standards were developed in line with HIQA's standards development process. The standard statements and features were informed by an evidence synthesis and consultation with an advisory group.

As a first step, the evidence synthesis was conducted, which included a detailed review of the international literature and an 'as-is' analysis of current structures and arrangements in Ireland for health and social care data. This review focused on legislation, standards, policy, guidelines and best practice in relation to health and social care data in other countries. The findings of this evidence synthesis enabled a gap analysis to be conducted, in order to identify where changes were required to the 2017 standards. This evidence synthesis is published on www.hiqa.ie.

An advisory group of experts and key stakeholders was convened by HIQA to provide advice and guidance on the development of these standards. The advisory group is made up of a diverse range of stakeholders, including Government departments, statutory bodies, professional groups, academia, and advocacy groups. Full details of the advisory group membership can be found in Appendix 1.

Structure of the draft national standards

The Draft National Standards for Information Management in Health and Social Care consist of three sections:

- Principles
- Standards
- Features

Principles

The standards are set out under the three principles of:

A rights-based approach: ensuring that data processing activities are conducted in accordance with the human rights principle of 'doing no harm'.

Accountability: ensuring that an organisation has all of the necessary governance arrangements in place to ensure its objectives in relation to data and information are met while adhering to all relevant legislation.

Responsiveness: ensuring that an organisation has arrangements in place to ensure it can adapt and respond to the changing health information landscape, takes a systematic approach to information governance, and ensures that maximum benefit is achieved from its data and information.

Standards

Each standard is comprised of two elements:

- A statement written from the perspective of an individual from which the data was collected regarding what they would expect from the organisation.
- A statement setting out the arrangements that an organisation that processes 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, demonstrate how an organisation can demonstrate that it is meeting the standard. The features detailed under each standard statement are not exhaustive and the organisation may meet the requirements of the standards in other ways.

Summary of the draft national standard statements

Principle 1: Rights-based approach	
Standard 1.1 People's rights relating to data and information	
What an individual should expect: I understand how the organisation collects, uses and shares my information, am confident that it has arrangements in place to protect my rights relating to information, and feel empowered to make decisions about my information.	**What an organisation should do to achieve this:** The organisation is transparent about how it collects, uses and shares information, and has effective arrangements in place to ensure individuals' rights under relevant legislation are upheld, balancing these rights against other values, fundamental rights, human rights, or legitimate, public or vital interests.
Standard 1.2 Privacy and confidentiality	
What an individual should expect: I am confident that the organisation has effective arrangements in place to ensure my privacy and confidentiality are respected when my information is being collected, used and shared.	**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 holds information.
Standard 1.3 Person-centred	
What an individual should expect: I am supported to be involved in making decisions about how my information is collected, used and shared, including getting access to, and using, my own information. I am confident that my wishes and priorities regarding my information are respected when possible.	**What an organisation should do to achieve this:** The organisation views the individuals about whom it holds information, including its staff members, as equal partners in planning, developing and monitoring its information management policies and processes to make sure their needs are met.

Principle 2: Accountability	
Standard 2.1 Organisational governance, leadership and management	
What an individual should expect: I am confident that the organisation has effective direction, and appropriate management and leadership arrangements in place, to ensure that information is collected, used and shared appropriately.	**What an organisation should do to achieve this:** The organisation has effective strategic governance, leadership and management arrangements in place with clear lines of accountability to ensure that information is collected, used and shared appropriately.
Standard 2.2 Strategy	
What an individual should expect: I am confident that the organisation has clear plans around information management and systems in order to deliver its services and meet its objectives.	**What an organisation should do to achieve this:** The organisation sets clear objectives in relation to the services that it provides and the associated information management and system requirements, and develops a clear plan for delivering on these objectives.
Standard 2.3 Performance assurance and risk management	
What an individual should expect: I am confident that the organisation has processes in place to assess its performance and manage risks relating to information management.	**What an organisation should do to achieve this:** The organisation has robust performance assurance and risk management policies in place in relation to information management to promote accountability to all stakeholders and encourage continuous and rigorous self-assessment.
Standard 2.4 Compliance with relevant legislation and codes of practice	
What an individual should expect: I am confident that the organisation is aware of all the relevant Irish and European law it has to follow and that my information is being collected, used and shared in a way that complies with all relevant legislation and codes of practice.	**What an organisation should do to achieve this:** The organisation is compliant with relevant Irish and European legislation and codes of practice, and has a process in place for identifying potential gaps in compliance with existing and forthcoming legislation.

Principle 3: Responsiveness	
Standard 3.1 Alignment with national and international standards and best practice	
What an individual should expect: I am confident that my information is managed by the organisation in line with national and international standards and best practice, incorporating any advancements in eHealth and information management.	**What an organisation should do to achieve this:** The organisation aligns with the latest national and international standards, policies and initiatives for safe and effective collection, use, sharing and dissemination of information, and strives to drive innovation in its information management practices.
Standard 3.2 Stakeholder engagement	
What an individual should expect: I am confident that the organisation has clear plans that set out how it will engage with all its stakeholders, including service users and members of the public, to identify their priorities and expectations, educate and empower them, and to plan for the organisation's current and future needs with regards to information management and the associated system requirements.	**What an organisation should do to achieve this:** The organisation takes a strategic approach to engaging with key stakeholders, including service users and members of the public, in order to identify its current and future needs and to be transparent about how information is used; it subsequently incorporates stakeholders' perspectives into its information management policies and processes and its outputs.
Standard 3.3 Use of information	
What an individual should expect: I am confident that the organisation uses information about me to its full potential and shares it in an appropriate way in order to inform decision-making and improve its services.	**What an organisation should do to achieve this:** The organisation uses information as a resource in planning, delivering, managing and improving its services, and has policies and processes in place to ensure information is shared and disseminated appropriately to protect the security, privacy and confidentiality of information and meet the needs of stakeholders.
Standard 3.4 Data quality	
What an individual should expect: I am confident that the organisation has policies and procedures in place to ensure a systematic approach to assessing, improving and maintaining the quality of its data to ensure it is 'fit for purpose'.	**What an organisation should do to achieve this:** The organisation takes a strategic approach to managing and improving data quality across the data and information lifecycle, and systematically assesses, documents and improves the quality of the data it holds through the use of a data quality framework.
Standard 3.5 Data security	
What an individual should expect: I am confident that my information is held safely and securely, and 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 information, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Principle 1: Human rights-based approach

In the context of health and social care information, the principle of a human rights-based approach relates broadly to ensuring that activities surrounding the collection, use and sharing of information are conducted in accordance with the human rights principle of 'doing no harm'.(15) Human rights are the basic rights and freedoms that all people should enjoy, and everyone is entitled to have their human rights respected and protected. A human rights-based approach is underpinned by a legal framework and human rights treaties which Ireland and other states have agreed to uphold.(16)

In the context of health information, a human rights-based approach means that an organisation places an emphasis on protecting and promoting people's rights relating to their information. This involves respecting their privacy and confidentiality, but also their autonomy, dignity, values, preferences and diversity. Data protection is a fundamental right set out in Article 8 of the EU Charter of Fundamental Rights.(17) Other specific rights of individuals in respect of their personal data under GDPR include, but are not limited to,: the right to access, the right to be informed (transparency), the right to rectification and the right to object.(18) 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 an obligation to balance these rights against other values, fundamental rights, human rights, and legitimate public or vital interests.

At a service provider level, an individual's health information informs all aspects of their care including assessment, diagnosis, treatment options and prognosis. It is essential, therefore, that service providers put in place arrangements to ensure that service users' information is managed appropriately and treated in a confidential manner. This includes having safeguards in place around access to information and ensuring that personal information is available to staff on an 'as-needs basis'. The underlying principles relating to privacy and confidentiality also apply to the secondary use of information, and all organisations need to find a balance between protecting the privacy of individuals and the use of information by putting in place the appropriate safeguards. Of note, however, is that it is necessary to consider the distinction between rights relating to personal data and aggregate data. For example, the level of safeguards in place for personal data may differ to those required for aggregate data, and organisations need to consider what safeguards are required to be in place at the different stages of the data and information lifecycle.

§ Equality means people having equal opportunities and being treated no less favourably than other people on the grounds set out in legislation. In an Irish context, these grounds are: age; civil status; disability; family status; gender; membership of the Traveller community; race, colour or nationality; religion or sexual orientation.

These safeguards should be clearly outlined within an organisation's privacy and confidentiality policies and procedures. Ongoing staff training in privacy and confidentiality is essential to ensure that staff working at all levels of an organisation understand their obligations relating to the protection of people's rights is an essential part of this.

By following a human rights-based approach to health information, an organisation is operating in a person-centred way. This means that the organisation views the individuals about whom it holds information, including its staff members, as equal partners in planning, developing and monitoring its information management policies and processes and has a clear focus on outcomes for those individuals.

Organisations should take a pro-active approach to engaging with the public and staff members, to identify their priorities and needs with regards to the information being collected and how it is used to facilitate informed decision-making and improve the safety and quality of services and population health and wellbeing. Services and organisations should also strive to work with people to ensure that necessary information is available in an accessible format.

Standard 1.1 People's rights relating to information

Standard 1.1	
What an individual should expect	**What an organisation should do to achieve this:**
I understand how the organisation collects, uses and shares my information, am confident that it has arrangements in place to protect my rights relating to information, and feel empowered to make decisions about my information.	The organisation is transparent about how it collects, uses and shares information, and has effective arrangements in place to ensure individuals' rights under relevant legislation are upheld, balancing these rights against other values, fundamental rights, human rights, or legitimate, public or vital interests.

Features of an organisation meeting this standard are likely to include:

1.1.1 Effective arrangements are in place, including clear policies and procedures that are **aligned with relevant Irish and European legislation and codes or practices**, for:

- Informing, and being transparent with, individuals about the extent to which their personal information is, or will be, collected, used or shared, as well as informing them about their rights relating to their information and what choices they have about this (see 1.2.1)
- Facilitating individuals to access a copy of their personal information in an accessible and timely way [**]
- Enabling individuals to have any factual inaccuracies in personal information held about them corrected, where certain conditions apply [††]
- Erasing personal information if an individual makes a request to have information held about them removed, where certain conditions apply [‡‡]
- Ensuring individuals can receive personal information in a format that makes it easier to re-use in another context, and to transfer it to another service or organisation, if such transfer is technically feasible.

[**] Under the GDPR, in limited circumstances, a request to access personal information may be refused.
[††] The right of rectification is restricted in certain circumstances under relevant Irish and European legislation.
[‡‡] The right to have your personal information erased is restricted in certain circumstances under relevant Irish and European legislation.

Standard 1.2 Privacy and confidentiality

Standard 1.2	
What an individual should expect:	**What an organisation should do to achieve this:**
I am confident that the organisation has effective arrangements in place to ensure my privacy and confidentiality are respected when my information is being collected, used and shared.	The organisation has effective arrangements in place to protect the privacy and confidentiality of people about whom it holds information.

Features of an organisation meeting this standard are likely to include:

1.2.1 The development and publication of a **Privacy Statement** which clearly outlines what information is collected, and how it is used and shared.

1.2.2 The use of **Data Protection Impact Assessments** (DPIAs), where relevant, to identify and mitigate any data protection-related risks arising from a new project. Where appropriate, the organisation should consider publishing the full DPIA or a summary.

1.2.3 Clear **policies and procedures** to ensure that any collection, use and sharing of personal information is adequate, relevant, and limited to what is necessary. This includes the development and implementation of:

- A Privacy and Confidentiality Policy and associated procedures
- Transfer of data policies and associated procedures, including information on the sharing or transfer of information within and between organisations, such as guidelines on appropriate de-identification techniques
- Data retention, archival, and destruction policies.

1.2.4 Ongoing training and updated guidance for staff and arrangements to ensure they are supported to understand their obligations relating to the protection of people's privacy and confidentiality rights.

Standard 1.3 Person-centred

Standard 1.3	
What an individual should expect:	**What an organisation should do to achieve this:**
I am supported to be involved in making decisions about how my information is collected, used and shared, including getting access to, and using, my own information. I am confident that my wishes and priorities regarding my information are respected when possible.	The organisation views the individuals about whom it holds information, including its staff members, as equal partners in planning, developing and monitoring its information management policies and processes to make sure their needs are met.

Features of an organisation meeting this standard are likely to include:

1.3.1 A clear focus on the **needs and preferences** of the individuals about whom it holds information, including its staff members, and the setting of objectives and plans that place individuals at the centre of all its information management policies and procedures.

1.3.2 Arrangements to ensure that individuals are confident their information is collected, used and shared in such a way that respects their **diversity**, including their life experience, age, gender, culture, language, beliefs and identity.

1.3.3 Arrangements to ensure that information is made available in an **accessible and timely** way, taking into account considerations such as potentials users' preferences and needs, disability, language, literacy levels and cultural background, to ensure that individuals can effectively co-ordinate, and make informed decisions about, their health and social care.

1.3.4 Arrangements are in place to ensure relevant stakeholders, including the public and staff members, are involved in the **co-design** of new health information initiatives or systems and as partners in the evaluation of any such initiatives or systems.

1.3.5 Arrangements to ensure that individuals have opportunities to provide **feedback** on the organisation's information management practices and the subsequent use of this feedback for regular evaluation of services and continuous improvement in this area to meet the identified needs and preferences of all.

Principle 2: Accountability

In the context of health and social care information, the principle of accountability relates broadly to organisations having the necessary governance arrangements in place to ensure its objectives in relation to data and information are met while adhering to all relevant legislation. An accountable organisation ensures that its services and objectives are planned in accordance with the assessed needs of the individuals about whom it holds information and follows a person-centred approach to optimise its information management practices. Achievement of high-quality information management practices is dependent on the culture of an organisation. The findings of a number of HIQA reviews of information management practices within the HSE have highlighted a need within the organisation for a strategic focus on information management at all levels, including effective leadership and oversight structures, in order to improve information management practices and optimise the use of information.[19-23]

Effective governance, leadership and management, in keeping with the size and complexity of the organisation and the type of services that it offers, are the organisational arrangements required to ensure that the objectives of the organisation in relation to its information management practices are met. Such arrangements ensure that appropriate processes, policies and procedures are developed, implemented and adhered to. A well-governed and managed organisation is clear about what it does and how it does it. Formalised governance arrangements ensure that there are clear lines of accountability at individual, team and organisational level 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. Senior management also have an important role to play in highlighting the need for, and importance of, high-quality health information in delivering high-quality, safe and reliable person-centred services and in strengthening and encouraging their organisation's culture in this regard.

The use of business and strategic plans can ensure that an organisation's objectives, purpose and strategy are clear and unambiguous. Developing and implementing business plans is essential for translating strategic plans into realistic work targets, and provides a basis to monitor progress to ensure that key outcomes are achieved within specified timelines. With regards to information management, a strategy that sets out how the organisation aims to improve the management of its information in order to achieve its overall strategic objectives may be outlined in the organisation's overall strategic plan or in a specific information management strategic plan. Regardless, these plans should be aligned with broader national and international health information strategies.

A well-governed and managed organisation can only be achieved if robust processes are in place to monitor performance. Senior management require information on how an organisation is performing to be assured that practices are consistently of a high standard. With regards to health information, this involves using selected key performance indicators 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.

There is also an onus on senior management to develop the required knowledge, skills and competencies within the organisation to manage information effectively and to ensure compliance with relevant Irish and European legislation. The enactment of the EU's GDPR in 2018, together with some key legislative changes in Ireland, including the 2018 Amendment to the Data Protection Act and the Health Research Regulations 2018, have had major implications for all organisations that process health and social care information. For example, the enactment of GDPR has provided further regulation and clarity regarding the legal bases for processing personal data, as well as the basic requirements for seeking valid consent. With further legislative changes imminent at both national and EU level, it is imperative that the organisations that process health and social care information have the appropriate expertise and policies and procedures in place to ensure they remain compliant.

Standard 2.1 Organisational governance, leadership and management

Standard 2.1	
What an individual should expect:	**What an organisation should do to achieve this:**
I am confident that the organisation has effective direction, and appropriate management and leadership arrangements in place, to ensure that 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.

Features of a service meeting this standard are likely to include:

2.1.1 **Clear lines of accountability** for all staff members, that are clearly documented and communicated throughout the organisation, to ensure a shared understanding of roles and responsibilities in relation to information management. This includes:

- an identified individual with overall accountability, responsibility and authority for information held by the organisation
- identified individuals or roles whose remit includes aspects of information management, for example: information governance, data quality, data security, data protection, and compliance with relevant legislation
- an organisational chart with roles and responsibilities clearly outlined.

2.1.2 A well-defined **governance and organisational structure** to ensure that the organisation's current and anticipated needs relating to information management are met in order to support effective decision-making and plan, design, manage and deliver services. This includes structures for oversight and day-to-day management of information management practices.

2.1.3 In situations where **joint governance arrangements** are required, the roles and responsibilities of each organisation are clearly outlined 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.

2.1.4 **Formalised 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 and generating of quality data. These could take the form of:

- Service-level agreements
- controller-processor contracts
- data sharing agreements

2.1.5 A **publicly available statement of purpose** that is in an accessible format; is reviewed regularly with input from relevant parties; is aligned with the overall strategy and direction of the organisation; and clearly and accurately outlines what the organisation sets out to achieve in terms of information management.

Standard 2.2 Strategy

Standard 2.2	
What an individual should expect:	**What an organisation should do to achieve this:**
I am confident that the organisation has clear plans around information management and systems in order to deliver its services and meet its objectives.	The organisation sets clear objectives in relation to the services that it provides and the associated information management and system requirements, and develops a clear plan for delivering on these objectives.

Features of an organisation meeting this standard are likely to include:

2.2.1 A **strategic plan** that sets clear direction for delivering on its objectives in relation to information management which is necessary for providing its services in the short, medium and long-term. Depending on the size and complexity of the organisation and the type of services that it offers, plans and specified objectives relating to information management should take account of:

- the organisation's overall strategic and business plans
- the organisation's current and future needs in relation to information management, including its technological and infrastructure requirements
- aspects of information governance, data security and data quality
- the use of information, including national reporting requirements
- national and international strategies, policies, standards and guidance relating to health information
- and the views and needs of all stakeholders, including members of the public.

2.2.2 Strategic **workforce planning** that takes account of the size, complexity and objectives of the organisation; the assessed needs of all stakeholders, including people using the service and people using the data; and the best available evidence.

2.2.3 Effective management of the **use of resources**, including human, physical, physical and information and communication technology (ICT) resources, to ensure continued sustainability.

2.2.4 Ongoing **training and professional development** opportunities for staff that are tailored to staff roles and responsibilities, and enable them to keep up to date with current and future information management practices.

Standard 2.3 Performance assurance and risk management

Standard 2.3	
What an individual should expect:	**What an organisation should do to achieve this:**
I am confident that the organisation has processes in place to assess its performance and manage risks relating to information management.	The organisation has robust performance assurance and risk management policies in place in relation to information management to promote accountability to all stakeholders and encourage continuous and rigorous self-assessment.

Features of an organisation meeting this standard are likely to include:

2.3.1 Regular review of performance relating to information management through an agreed **performance assurance framework** to include roles and responsibilities of committees, management and staff.

2.3.2 Arrangements to measure and report on performance using **key performance indicators (KPIs)** that are regularly reviewed to ensure they are relevant, reliable and accurate.[§§]

2.3.3 A schedule of **internal and external audits** to assess compliance with relevant legislation and the organisation's information management policies and procedures.

2.3.4 Policies and processes for **risk management**, including regular review of the risk management policy and risk register, to ensure that all risks, including risks relating to individuals' privacy and confidentiality, data security, data quality, and use of information are assessed and managed appropriately.

2.3.5 A process for capturing positive and negative **feedback**, including a formal complaints procedure for reviewing and investigating complaints received related to information management.

[§§] A systematic process is required to identify appropriate KPIs for an organisation, and ongoing monitoring and review is essential to ensure the most relevant KPIs are being used and reported on. In order to report on KPIs and use them effectively, it is essential that the correct data is being collected and that good information management practices are being adhered to.

Standard 2.4 Compliance with relevant legislation and codes of practice

Standard 2.4	
What an individual should expect:	**What an organisation should do to achieve this:**
I am confident that the organisation is aware of all the relevant Irish and European law it has to follow and that my information is being collected, used and shared in a way that complies with all relevant legislation and codes of practice.	The organisation is compliant with relevant Irish and European legislation and codes of practice, and has a process in place for identifying potential gaps in compliance with existing and forthcoming legislation.

Features of an organisation meeting this standard are likely to include:

2.4.1 Identified individuals to perform key roles that are outlined in relevant legislation, including that of a **data protection officer**.

2.4.2 Clearly documented and implemented arrangements to provide assurance of, awareness of, and compliance with, relevant existing and forthcoming **Irish and European legislation and codes of practice**. This includes:

- an identified individual or role with responsibility for leading the process of continually reviewing and identifying gaps in compliance with existing and forthcoming legislation, and for developing processes for achieving compliance in a timely way following the identification of any gaps or compliance issues
- documented processes and procedures for the receipt, sharing and release of information in line with relevant legislation
- documented processes to illustrate a continuous review of data protection related risks
- documented and implemented processes to be undertaken if there is a suspected or actual breach of legislation

2.4.3 Regular and ongoing **training** to ensure that staff are aware of, and adhere to, the legislation and codes of practice relevant to their role.

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. It also means having the appropriate arrangements and safeguards in place to ensure that individuals are assured that their information is being managed in a safe and secure way. Furthermore, responsiveness means ensuring the organisation is aligned with best practices nationally and internationally, drives innovation, and ensures maximum benefit is achieved from information, through using and sharing it appropriately for both primary and secondary purposes.

All organisations that process health and social care information need to be responsive to the significant changes occurring in this area nationally and internationally, including developments with the establishment of the European Health Data Space. Organisations should be ready to adapt and ensure compliance with any forthcoming changes to national and international policy and legislation, as well as any relevant health information standards, policies and initiatives which may impact on the interoperability of systems and the sharing and re-use of health and social care information.

Effective stakeholder engagement is a key feature of a person-centred organisation and also underpins a human rights-based approach to health information. It involves facilitating and encouraging active participation of all relevant stakeholders, including people using services and the general public. In the context of health and social care information, meaningful stakeholder engagement ensures that individuals about whom the information relates, as well as other key users of the information, are given the opportunity to express their needs, preferences and expectations about the information that the organisation holds.

To effectively use information, organisations need systems, including information and communication technology (ICT) systems, in place to ensure suitable practices are in place for its collection, use and sharing. All staff should have access to the information that they need when they need it to facilitate effective decision-making. At a service level, a service user's health information informs all aspects of their care, including assessment, diagnosis, treatment options and prognosis. As such, it is vital that once information is collected, it is available to staff to support effective decision-making at the point of care. For those involved in managing the health and social care system at local and national levels, as well as policy-makers, researchers and other key data users, the availability of information in an accessible and timely way, with all the appropriate safeguards in place, optimises its use and increases the potential outputs that can be achieved.

Quality information is an important resource for organisations in planning, managing, delivering and monitoring high-quality services. It is also essential that senior managers and decision-makers are assured of the quality of information upon which key decisions are being based. High-quality information can be achieved through an organisation using a systematic approach to assessing, improving and maintaining the quality of its information to ensure it is 'fit for purpose'. HIQA's guidance on a data quality framework outlines how organisations can use internationally recognised dimensions*** to assess quality across all stages of the data and information lifecycle. This enables organisations to apply a framework to help assess and improve data quality on a continuous basis and to ensure learning is incorporated in effective changes in practice, policies or procedures.

Data and information security in the context of health and social care is a rapidly evolving field and should be embedded in to the culture of an organisation. The cyber-attack on the HSE's information IT systems in 2021 caused significant and prolonged disruption to the health and social care system and highlighted the need for major change. The findings and recommendations from an independent, commissioned report have led to some changes in the HSE's cyber security structures and processes with a view to implementing a multi-year ICT and cybersecurity transformation programme across the organisation.(24) It is of upmost importance, therefore, that a strategic and proactive approach is taken to data and information security.

*** Internationally recognised dimensions to assess data and information quality include: relevance; accuracy and reliability; timeliness and punctuality; coherence and comparability; and accessibility and clarity.

Standard 3.1 Alignment with national and international standards and best practice

Standard 3.1	
What an individual should expect:	**What an organisation should do to achieve this:**
I am confident that my information is managed by the organisation in line with national and international standards and best practice, incorporating any advancements in eHealth and information management.	The organisation aligns with the latest national and international standards, policies and initiatives for safe and effective collection, use, sharing and dissemination of information, and strives to drive innovation in its information management practices.

Features of an organisation meeting this standard are likely to include:

3.1.1 Regular review of national and international **standards, guidance and recommendations** that are formally issued by regulatory bodies in order to determine what is relevant to the organisation, and a process for taking the necessary actions to address any identified gaps. This might include:

- Health information and technical standards to support or enable the interoperability of systems
- Guidance relating to the use of unique health identifiers
- Guidance relating to data linkage.

3.1.2 Effective arrangements to ensure **adherence to**, and to demonstrate **compliance with**, relevant standards, where appropriate.

3.1.3 Effective use of the latest **information and communication technology (ICT) resources** for all aspects of data and information management, including data quality and validation, data dissemination and data security, incorporating any new and upcoming advancements in ICT resources and eHealth.

Standard 3.2 Stakeholder engagement

Standard 3.2	
What an individual should expect:	**What an organisation should do to achieve this:**
I am confident that the organisation has clear plans that set out how it will engage with all its stakeholders, including service users and members of the public, to identify their priorities and expectations, educate and empower them, and to plan for the organisation's current and future needs with regards to information management and the associated system requirements.	The organisation takes a strategic approach to engaging with key stakeholders, including service users and members of the public, in order to identify its current and future needs and to be transparent about how information is used; it subsequently incorporates stakeholders' perspectives into its information management policies and processes and its outputs.

Features of an organisation meeting this standard are likely to include:

3.2.1 A **strategy and plan** for engaging with key stakeholders, including people using services, members of the public, staff and other users of the data. These should include details of how the organisation will achieve the following:

- identify **priorities** and **expectations** of key stakeholders, with regards to health information
- identify what information it should be collecting and reporting on, such as **equity stratifiers** and the most appropriate and meaningful **indicators of patient safety and quality of care** outcomes
- **educate** individuals on their rights relating to their health information, including what choices are available
- **empower** individuals to make informed choices about the uses of their health information, including educating them on the benefits and risks associated with sharing their data
- work with key stakeholders to develop **plans** for the organisation with respect to health information, including the current and future information management needs of the organisation, and how best to present its data and reports.

Standard 3.3 Use of information

Standard 3.3	
What an individual should expect:	**What an organisation should do to achieve this:**
I am confident that the organisation uses information about me to its full potential and shares it in an appropriate way in order to inform decision-making and improve its services.	The organisation uses information as a resource in planning, delivering, managing and improving its services, and has policies and processes in place to ensure information is shared and disseminated appropriately to protect the security, privacy and confidentiality of information and meet the needs of stakeholders.

Features of an organisation meeting this standard are likely to include:

3.3.1 Arrangements to ensure that high-quality information is **available** and **shared**[†††] in a timely way within, and between, organisations in line with legislation, to facilitate the use of information to support effective clinical and personal decision-making, monitor the safety and quality of care, and for other secondary purposes. These arrangements might include:

- policies and procedures that clearly document staff roles and responsibilities with regards to the routine sharing of information within and between organisations for both primary and secondary uses
- policies and procedures, as well as accessible guidance for potential data users, with regards to specific requests for information
- a plan for the effective sharing of information that is incorporated in to the overall strategy of the organisation and informed by the FAIR Guiding Principles of findability; accessibility; interoperability; and reusability(25)
- procedures to assess and manage risks associated with information sharing that are informed by the dimensions of the Five Safes framework: safe data; safe projects; safe people; safe settings; and safe outputs.(26)

3.3.2 Arrangements to ensure that information is **disseminated**[‡‡‡] in a timely and accessible way, in order to deliver maximum public benefit by assisting individuals and other key stakeholders to make informed and evidence-based decisions.

[†††] *Data sharing* refers to making data available to another agency, organisation or person under agreed conditions.
[‡‡‡] *Data dissemination* refers to 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.

3.3.3 Arrangements to ensure that information management **systems**, whether electronic or paper-based, are integrated and supported by other systems where possible, and used effectively to collect, use, share and disseminate information as appropriate to support effective clinical and personal decision-making and to facilitate the optimal use of information for secondary purposes. This might include:

- the development and maintenance of resources to support the needs of the public and other stakeholders, such as web-based tools for accessing and using health information
- the submission of data to Ireland's Open Data portal
- the creation of a secure environment for the safe linkage, analysis, management and storage of personal data.

3.3.4 Routine **monitoring** of the use of information for relevance and usability and a plan to address any identified areas for improvements.

Standard 3.4 Data quality

Standard 3.4	
What an individual should expect:	**What an organisation should do to achieve this:**
I am confident that the organisation has policies and procedures in place to ensure a systematic approach to assessing, improving and maintaining the quality of its data to ensure it is 'fit for purpose'.	The organisation takes a strategic approach to managing and improving data quality across the data and information lifecycle, and systematically assesses, documents and improves the quality of the data it holds through the use of a data quality framework.

Features of an organisation meeting this standard are likely to include:

3.4.1 An **identified individual** or role whose remit includes systematically assessing, monitoring and reviewing data quality.

3.4.2 The use of **a data quality framework** that outlines the approaches to assure the quality of data by assessing, documenting and improving data quality in a standardised way.[§§§] This should include the following components:

- A **Data Quality Strategy**, which set 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**, which comprises a set of criteria to comprehensively assess data sources across the five dimensions of data quality.[****]
- **Data quality reports**, which could include internal or external data quality assessment reports, reports on key performance indicators or metrics, and the production of 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.

[§§§] For further guidance, see: Health Information and Quality Authority (2018) *Guidance on a data quality framework for health and social care*, available on HIQA's website: www.hiqa.ie
[****] These are relevance; accuracy and reliability; timeliness and punctuality; coherence and comparability; accessibility and clarity.

3.4.3 A comprehensive mapping of **data flows** which details all data entering and leaving the organisation, including a written record of all data processing activities, 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.

3.4.4 Well-defined **policies and procedures** in relation to the quality of data that address each dimension of data quality and consider all stages of the data and information lifecycle that apply to the organisation, including the following:

- **Capture:** established processes to ensure consistency in data collection and acquisition, including the use of a data dictionary and classification systems and clinical terminologies, for example ICD-10 and SNOMED-CT.
- **Submission:** established mechanisms for submitting data to an organisation, including the use of standards, submission specifications and tools.
- **Processing:** protocols for the routine review of data when it is acquired, including automated or manual quality control checks, and data validation and audits to check the completeness and correctness of data.
- **Analysis:** data analysis plans that take into account any identified or potential data quality issues.
- **Dissemination:** consideration of any data quality issues when the data is being disseminated, including the publication of a data quality statement with all published outputs.

3.4.5 Ongoing data quality training for staff, that is informed by data quality audits and the best available evidence, in order to promote data quality awareness and prevent the occurrence of errors.

Standard 3.5 Data security

Standard 3.5	
What an individual should expect:	**What an organisation should do to achieve this:**
I am confident that my information is held safely and securely, and my confidentiality is protected.	The organisation has effective physical and technical security arrangements in place to ensure the confidentiality, integrity and availability of information, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Features of an organisation meeting this standard are likely to include:

3.5.1 Strong **accountability and governance arrangements** are in place to support robust data protection and data security structures, including:

- Clear lines of **accountability**, including an identified individual or role with ultimate responsibility for implementation and oversight of data security policies
- Input and support from **external** agencies where adequate data security expertise is not available internally
- **Future planning** to identify and respond to new or potential security risks
- Regular **reporting** to demonstrate the extent to which the organisation is assured of its data security arrangements.

3.5.2 Robust **assurance and review** policies and processes for investigating and responding to potential security risks and ensuring information is always adequately protected, including:

- A **data security policy** that is aligned with national and international best practice, linked to the organisation's risk register and embedded in to the risk assessment cycle
- **Security risk assessments** to identify, analyse and evaluate physical and technical security risks and determine practical steps to minimise the risks
- A schedule of **internal and external audits** to assess compliance with the organisation's policies and procedures relating to data security and to systematically identify opportunities to improve data security practices
- Policies and processes to be followed in the event of a **data protection breach**.

3.5.3 Adequate physical and technical environments to ensure information is **stored** in a secure and suitable way that prevents unauthorised access and ensures it is accessible and retrievable for as long as required.

3.5.4 **Role-based access controls**, whereby access to information is granted on a needs basis. A record of staff, including their roles and their levels of access, should be maintained.

3.5.5 Clear plans which are regularly tested and outline the processes to follow in the event of a **systems failure or significant data security breach**, including:

- Business continuity plan
- Disaster recovery plan.

3.5.6 Employees and contractors receive **ongoing training** in data security and cyber awareness, and are supported to understand their obligations relating to data security, integrity and honesty.

References

1. Health Act 2007 (Ireland). Available from: https://www.irishstatutebook.ie/eli/2007/act/23/enacted/en/html. Accessed on: 12 September 2022.

2. Health Information and Quality Authority. *The need to reform Ireland's national health information system to support the delivery of health and social care services.* Dublin: 2021. Available from: https://www.hiqa.ie/sites/default/files/2021-10/The-need-for-reform-of-the-health-information-system.pdf. Accessed on: 28 October 2021.

3. 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: 6 December 2021.

4. New Zealand Government. (2022) *Data Toolkit* [Online]. Available from: https://www.data.govt.nz/toolkit/. Accessed on: 10 June 2022.

5. European Medicines Agency. *Patient Registry Initiative- Strategy and Mandate of the Cross-Committee Task Force*. 2017. Available from: https://www.ema.europa.eu/en/documents/other/patient-registry-initiative-strategy-mandate-cross-committee-task-force_en.pdf. Accessed on: 5 July 2022.

6. Health Information and Quality Authority. *Guidance on information governance*. Dublin: 2012. Available from: https://www.hiqa.ie/reports-and-publications/health-information/guidance-information-governance-health-and-social-care. Accessed on: 13 June 2022.

7. Houses of the Oireachtas. *Committee on the Future of Healthcare - Slaintecare Report*. Dublin: 2017. Available from: https://data.oireachtas.ie/ie/oireachtas/committee/dail/32/committee_on_the_future_of_healthcare/reports/2017/2017-05-30_slaintecare-report_en.pdf. Accessed on: 4 March 2022.

8. Department of Health. *Sláintecare Implementation Strategy & Action Plan 2021 — 2023*. Dublin: 2021. Available from: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjv2vC4rKz2AhXUMMAKHfe3CMsQFnoECAMQAQ&url=https%3A%2F%2Fassets.gov.ie%2F134746%2F9b3b6ae9-2d64-4f87-8748-cda27d3193f3.pdf&usg=AOvVaw3hWyevDq3-36aGpL_5yph4. Accessed on: 7 July 2022.

9. General Data Protection Legislation 2018 (European Union). Available from: https://gdpr-info.eu/. Accessed on: 28 October 2021.

10. Data Protection Act 2018 (Ireland). Available from: https://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html. Accessed on: 28 October 2021.

11. Data Protection Act 2018 (Section 36(2)) (Health Research) Regulations 2018 (Ireland). Available from: https://www.irishstatutebook.ie/eli/2018/si/314/made/en/print. Accessed on: 28 October 2021.

12. Health Research Consent Declaration Committee. (2022) *HRCDC - Overview* [Online]. Available from: https://hrcdc.ie/about-us/. Accessed on: 22 September 2022.

13. Child Care Act 1991 (Ireland). Available from: https://www.irishstatutebook.ie/eli/1991/act/17/enacted/en/html. Accessed.

14. Children Act 2001 (Ireland). Available from: https://www.irishstatutebook.ie/eli/2001/act/24/enacted/en/html. Accessed on: 13 October 2022.

15. United Nations. *A human rights-based approach to data*. Geneva: 2018. Available from: https://www.ohchr.org/sites/default/files/Documents/Issues/HRIndicators/GuidanceNoteonApproachtoData.pdf. Accessed on: 10 June 2022.

16. Health Information and Quality Authority. *Guidance on a Human Rights-based Approach in Health and Social Care Services*. Dublin: 2019. Available from: https://www.hiqa.ie/reports-and-publications/guide/guidance-human-rights-based-approach-health-and-social-care-services. Accessed on: 9 September 2022.

17. 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: 8 June 2022.

18. Data Protection Commission. (2022) *Your Rights under the GDPR* [Online]. Available from: https://www.dataprotection.ie/en/individuals/rights-individuals-under-general-data-protection-

regulation#:~:text=Everyone%20has%20the%20right%20to,basis%20laid%20down%20by%20law. Accessed on: 8 June 2022.

19. Health Information and Quality Authority. *Review of information management practices at BreastCheck*. Dublin: 2018. Available from: https://www.hiqa.ie/sites/default/files/2018-03/Review-nformation-management-practices-BreastCheck_March-2018.pdf. Accessed on: 2 March 2022.

20. Health Information and Quality Authority. *Review of information management practices for the National Incident Management System (NIMS) within the HSE*. Dublin: 2021. Available from: https://www.hiqa.ie/sites/default/files/2021-05/Review-of-information-management-practices-for-the-National-Incident-Management-System-(NIMS)-within-the-HSE.pdf. Accessed on: 2 March 2022.

21. Health Information and Quality Authority. *Review of information management practices in the Hospital In-Patient Enquiry (HIPE) scheme*. Dublin: 2018. Available from: https://www.hiqa.ie/sites/default/files/2018-10/HIPE-report.pdf. Accessed on: 2 March 2022.

22. Health Information and Quality Authority. *Review of information management practices in the HSE Computerised Infectious Disease Reporting (CIDR) system*. Dublin: 2019. Available from: https://www.hiqa.ie/sites/default/files/2019-11/Review%20of%20information%20management%20practices%20in%20the%20CIDR%20system.pdf. Accessed on: 2 March 2022.

23. Health Information and Quality Authority. *Review of information management practices in the HSE Primary Care Reimbursement Service (PCRS)*. Dublin: 2019. Available from: https://www.hiqa.ie/sites/default/files/2019-03/Review-of-information-management-practices-in-the-hse-Primary-Care-Reimbursement-Service-(PCRS).pdf. Accessed on: 2 March 2022.

24. Price Waterhouse Cooper. *Conti cyber attack on the HSE - Independent Post Incident Review*. Dublin: 2021. Available from: https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf. Accessed on: 22 September 2022.

25. Wilkinson, M. D., Dumontier, M., Aalbersberg, I. J., Appleton, G., Axton, M., Baak, A., et al. The FAIR Guiding Principles for scientific data management and stewardship. *Scientific data*. 2016; 3:[160018 p.].

26. Desai, T., Ritchie, F., Welpton, R. *Five Safes: designing data access for research*. Bristol: 2017. Available from: https://core.ac.uk/download/pdf/323894811.pdf. Accessed on: 21 December 2021.

Appendix 1. Advisory group membership **

Name	Organisation - *Title*
Azul O' Flaherty	Department of Health - *Assistant Principal, Health Information Policy Unit*
Cliona 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 - *Coding Manager*
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*
Michael Courtney	Department of Health - *Statistician*
Michael Power	HSE National Patient and Service User Forum - *Member*
Sandra Ryan	Office of the Chief Information Officer, HSE - *Technical Standards Lead*
Selina Ryan	Health Informatics Society of Ireland (HISI) - *Nurse Lead for Informatics, St James Hospital*
Simon Woodworth	University College Cork - *Director, Health Information Systems Research Centre*
Sarah Craig	Health Research Board - *Head of National Health Information Systems*
Tibbs Pereira	Patients for Patients Safety Ireland - *Member*
Trevor Duffy	Royal College of Physicians in Ireland - *Director of Healthcare Leadership*

** Additional members are currently being invited to join the advisory group to increase representation; this process is ongoing.

Published by the Health Information and Quality Authority (HIQA).

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