Health Information and Quality Authority

An tÚdarás Um Fhaisnéis agus Cáilíocht Sláinte

Guidance on information governance for health and social care services in Ireland

Safer Better Care

About the Health Information and Quality Authority

The Health Information and Quality Authority (HIQA) is the independent Authority established to drive continuous improvement in Ireland's health and personal social care services, monitor the safety and quality of these services and promote person-centred care for the benefit of the public.

The Authority's mandate to date extends across the quality and safety of the public, private (within its social care function) and voluntary sectors. Reporting to the Minister for Health and the Minister for Children and Youth Affairs, the Health Information and Quality Authority has statutory responsibility for:

- **Setting Standards for Health and Social Services** – Developing person-centred standards, based on evidence and best international practice, for those health and social care services in Ireland that by law are required to be regulated by the Authority.
- **Social Services Inspectorate** – Registering and inspecting residential centres for dependent people and inspecting children detention schools, foster care services and child protection services.
- **Monitoring Healthcare Quality and Safety** – Monitoring the quality and safety of health and personal social care services and investigating as necessary serious concerns about the health and welfare of people who use these services.
- **Health Technology Assessment** – Ensuring the best outcome for people who use our health services and best use of resources by evaluating the clinical and cost effectiveness of drugs, equipment, diagnostic techniques and health promotion activities.
- **Health Information** – Advising on the efficient and secure collection and sharing of health information, evaluating information resources and publishing information about the delivery and performance of Ireland's health and social care services.

Table of Contents

1. Introduction

Providing high quality and safe health and social care relies on good use of, access to, and appropriate sharing of, high quality information.

Good information governance practices support and promote increased confidence among people who use health and social care services in the service provider's ability to manage their information. They are, therefore, more likely to provide up-to-date, accurate information, which ultimately improves the quality of care and services that they receive. This also promotes trust among health and social care professionals who can confidently rely on having access to good quality information to support decision making.

Ultimately, good information governance practice is about complying with the law in relation to information handling practices.

This guidance is the first in a series of guidance documents from the Health Information and Quality Authority (HIQA) aimed at supporting the successful implementation of the *National Standards for Safer Better Healthcare* (the National Standards) published by HIQA in June 2012. The purpose of the guidance is to:

- facilitate the successful implementation of the National Standards
- provide common understanding and language across all healthcare services
- provide examples from different services of steps that providers can take to meet the National Standards.

The *National Standards for Safer Better Healthcare* are structured around eight themes for quality and safety (Figure 1).

Figure 1: Themes for Quality and Safety

As Figure 1 illustrates, the eight themes are intended to work together. Collectively, they describe how a service provides high quality, safe and reliable care centred on the service user. The four themes on the upper half of the figure, relate to dimensions of quality and safety and the four on the lower half of the figure, relate to key areas of capacity and capability.

Theme 8 of the National Standards, **Use of Information**, identifies that quality information is an important resource for service providers in planning, managing, delivering and monitoring high quality safe services. Good information governance enables services and individuals to ensure all information, including personal information, is handled securely, efficiently, effectively and in line with legislation. This supports the delivery of person-centred, safe, high quality health and social care and helps ensure that when sharing information across services, service providers protect and manage personal information in a sensitive and responsible manner.

This document, *Guidance on information governance for health and social care services in Ireland*, has been developed to support senior managers working in health and social care, regardless of the service, setting or location, to collect, analyse, use and share personal health information legally, securely, effectively and efficiently.

This guidance document is a useful resource for all senior managers and staff who are responsible for handling such information in the provision of health and social care services. It is aimed specifically at managerial level as a resource to implement information governance in their organisations.

For the purpose of this guidance the term 'organisation', 'service' or 'service providers' can be taken to mean a health or social care organisation, setting or service for example hospitals, ambulance services, residential services for older people or foster care services.

1.1 Structure and function of the guidance

This document gives guidance on implementing an appropriate governance and management structure to support information governance and then gives additional detail on data quality, privacy and confidentiality, information security and secondary use of information; and provides examples for service providers in relation to each of these.

The examples are practical steps to be taken in implementing information governance practices and in ensuring compliance with information governance requirements. The guidance does not contain an exhaustive list of examples nor are they designed to be a checklist for compliance with information governance requirements. Service providers may choose different approaches to meet their responsibilities in relation to the management of personal health information. The examples outlined in this document provide high-level guidance, and implementation will involve providers developing local implementation plans based on their respective service, setting or location.

Some of the examples contained in this guidance may require additional resources, for instance training and education, however, many do not and can be adopted simply by changing the way in which information is handled. For example, registering with the Data Protection Commissioner, informing service users about the use of their information through a statement of information practices,* incorporating a confidentiality agreement into all contracts of employment and formal contractual arrangements will require minimal resources to implement. Details of what should be contained in a statement of information practices are outlined in Appendix 1.

* A statement of information practices is a generic document made available to service users, for example by displaying it in waiting rooms or at reception desks. It should set out, at a high level, what information the service collects, how it is used, with whom it is shared and for what purpose, the safeguards that are in place to protect it and how service users can access information held about them.

2. Information Governance

2.1 What is personal health information?

Data can be defined as raw facts and statistics before they have been organised or put into context. Once data are collated and analysed to produce something useful, they then become information. Personal health information is defined as information, recorded in any form or medium, which is created or communicated by an organisation or individual relating to the past, present or future care of an individual or cohort. Personal health information is data relating to an individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller.[1] The term personal health information is broad and includes such matters as personal information relating to the physical or mental health of the individual, as well as any genetic data or human tissue data that could be predictive of the health of the individual or his or her relatives or descendants. In essence it covers any information relating to an individual that is collected for or in connection with the provision of a health or social care service.

For the purpose of this guidance the term 'personal health information' includes information relating to an individual's health and social care. It also includes information in the possession of health and social care services in relation to services and the health and welfare of the general population.

2.2 What is information governance?

Information governance provides a means of bringing together all the relevant legislation, guidance and evidence-based practice that apply to the handling of information and offers a consistent way for people working in health and social care to deal with the many different legal provisions, guidance, and professional codes of conduct that apply to handling personal health information.

Good information governance enables personal health information, such as that contained in a health or social care record, to be handled legally, securely, efficiently and effectively in order to deliver the best possible care to people who use health and social care services. It also includes the appropriate sharing of relevant personal health information between health and social care professionals involved in the provision of care with a view to informing the development of this care.

Information governance involves the development of processes and procedures for handling personal health information that support the efficient location and retrieval of records where and when they are needed. It is about setting a high standard for the handling of personal health information and giving staff and service providers the tools they need to achieve that standard.

All staff in health and social care settings handle personal health information in some way and therefore information governance is everyone's responsibility. Senior management have a specific role to play in information governance through the

development and implementation of staff training, policies and procedures and generally promoting and supporting a culture of good information governance. Ultimately, responsibility and accountability for information governance rests with the chief executive officer (CEO) or equivalent within the organisation.

Robust information governance practices facilitate:

- The collection of high **quality data** to meet the requirement of data users to support service delivery, quality improvement, performance reporting and planning. This refers to data that is accurate, valid, reliable, timely, relevant, legible and complete.
- The maintenance of **privacy and confidentiality** of individuals. This is driven by the requirements of the Data Protection Acts 1988 and 2003[1;2] and the Freedom of Information Acts 1997 and 2003.[3;4] Privacy can be defined as the right of individuals to keep information about them from being disclosed. Confidentiality refers to a duty that a person owes to safeguard information that has been entrusted to him or her by another.
- **Information being held securely**. Information security is concerned with having systems in place to ensure that all information is held confidentially and securely, can be relied upon in use, and is available to authorised persons when and where needed.[5] It is concerned not only with technical methods for securing information but also deals with physical and behavioural security measures.
- The appropriate safeguards for the **secondary use of information** being in place to protect the individual's rights to privacy and confidentiality. This relates to the appropriate use of information which has been collected in the course of providing care for purposes other than direct care. Service-user data can be used for many valuable secondary purposes, which bring benefits to the service-user population as a whole. These secondary uses include clinical research, public health, epidemiology, audit and quality assurance, service planning and regulatory and monitoring activities.

Formalised governance arrangements are essential for information governance. This ensures that there are clear lines of accountability at individual, team and service levels so that health and social care professionals, managerial staff and everyone working in the service are aware of their responsibilities and their accountability for information governance. These governance and management arrangements should be appropriate for the size, scope and complexity of the service provided which allow for accountability, decision making and risk management for information governance. Governance and management structures to support information governance include the following:

- having executive level responsibility, accountability, leadership and effective management in place to allow organisations to be clear about who does what, make decisions and risk manage information governance

- standardised information governance policies and procedures developed in accordance with legislation and best available evidence for staff to follow
- a fully trained and educated workforce with the necessary skills and competencies to support information governance
- improvements in information governance on a continuous basis, leading to improvements in the quality of care being provided.

The next section provides guidance on the necessary governance and management structures to support information governance in order to collect high quality data, ensure individuals' privacy is maintained, information is held securely, and the appropriate safeguards are in place for secondary use of information. Each of following areas is further explored in more detail and examples of them are given:

- data quality
- privacy and confidentiality
- information security
- secondary use of information.

For more information on information governance and the role of the Health Information and Quality Authority in this area see Appendix 2.

2.3 Governance and management structures to support information governance

2.3.1 What are governance and management structures?

In order to develop good information handling practices throughout a service, it is necessary to have structures and processes in place to provide direction to staff on information governance. Responsibility and accountability for information governance must be clearly defined and this can be achieved through the service's governance structure.

Appropriate governance and management structures are required, which are part of the overall governance structure, including clinical governance, to support information governance within a service. Formalised governance arrangements ensure that there are clear lines of accountability at individual, team and management levels so that everyone working in the service is aware of their responsibilities and accountability. Identified staff members should have responsibility for information governance within a service and all staff members should be adequately informed of and trained in their responsibilities in this regard.[5]

Governance and management arrangements encompass the structures and the development and implementation of policies and procedures relating to all aspects of

information governance, the continued assessment of compliance with these policies and procedures and development of improvement plans as appropriate.

2.3.2 Why is it important to have governance and management structures in place to support information governance?

Governance and management structures are the overarching elements to information governance that enable quality data, privacy and confidentiality and security of personal health information and information used for secondary purposes. This supports good information governance practices by:

- setting out the service's accountability arrangements for information governance as part of the service's overall governance structures so that all staff and management are aware of their responsibilities
- supporting staff, including managers and clinicians, to do the right thing or make the right decision at the right time
- embedding a culture of good information governance throughout the service
- promoting and supporting continuous improvements in the delivery of quality, safe and reliable health and social care services.

Governance and management structures to support information governance include having:

- executive level responsibility, accountability, leadership and effective management
- policies and procedures
- training and education
- self-assessment and continuous improvement.

Each of these is relevant to support data quality, privacy and confidentiality, information security and the secondary use of information.

2.3.3 Executive level responsibility, accountability, leadership and effective management

Executive level responsibility, accountability, leadership and effective management are necessary to allow organisations to be clear about who does what, make decisions and risk manage information governance. Accountability for information governance should be assumed at the most senior level within a service. Responsibility for information governance practices within a service should be delegated to senior management reporting through the normal governance

arrangements of the service. A well governed and managed service monitors its performance to ensure that it manages information to a high standard that is consistent across the service. Leadership, governance and management arrangements involve creating a culture within a service to enable staff to fulfil their roles and responsibilities, either individually or as members of a team.

It is important that service users are confident that management arrangements support the collection, storage and use of personal information efficiently, effectively and securely. How information is governed in an organisation should be documented and approved at the most appropriate senior level, this document should be regularly reviewed and updated as appropriate. It should detail roles and responsibilities in relation to data quality, privacy and confidentiality, information security and secondary use of information throughout the service.

It is important that service users are confident of the governance and management arrangements in place to support their information being held securely and protected from loss, theft, corruption and inappropriate access and to support the appropriate use of their information for secondary purposes. These arrangements enable senior management to be fully informed of and accountable for the ways in which information is used.

For example

- Service providers document how information is governed as part of the service's overall governance structure which is approved at the most appropriate senior management level. This should be regularly reviewed and updated to comply with relevant legislation, standards and guidance and includes clear reporting and accountability arrangements.
- Service providers have clearly stated levels of responsibility and accountability for information governance within the service and this is communicated at every level of the service from front-line staff to senior level decision makers.
- There is a named senior individual who is responsible and accountable for information governance who reports formally through the service provider's governance structures. This individual receives appropriate support and training to fulfil this role.
- The accountability arrangements in a service are regularly reviewed to ensure that they are robust and effective and that everyone working in the service understands their role and responsibilities regarding information governance.

- The service provider is registered, where required, with the Data Protection Commissioner outlining the purpose for holding personal information and ensures that information provided to the Data Protection Commissioner is updated as necessary.
- Service providers ensure there are appropriate procedures in place for transferring data outside of the service, including additional safeguards for transfer outside of the European Economic Area (EEA) as set out in Data Protection legislation.
- There is a process for reporting information governance performance to management. These reports are part of standard risk management arrangements and the service's overall performance reporting. The implications of poor performance are managed.
- Strategic and business plans incorporate current and future needs for information governance objectives.
- The workforce is configured and managed in such a way that there are sufficient numbers of suitably qualified individuals to assess, document and address information governance effectively.
- Job descriptions, employment contracts and formal contractual arrangements include the need for compliance with information governance policies and procedures by all individuals, groups and organisations carrying out work on behalf of the health and social care service. This includes signing a confidentiality agreement.
- Information governance is incorporated into the performance appraisal process.
- There is a process in place to deal with breaches of information governance policies and procedures, which involves service providers monitoring and reviewing adverse incidents relating to information governance and ensuring that effective remedial and preventative action is taken.
- Service providers are aware of all secondary uses of information within the service involving information collected or held by the service and are responsible for ensuring compliance with relevant legislation for all uses, including responding to external requests for information and are accountable for each of these uses.
- Where there is a legal basis for using information for secondary purposes, service providers incorporate requirements concerning the secondary use of information into formal agreements for joint working with external organisations/agencies and individuals. This includes having data sharing agreements in place with organisations that they routinely share information

with requiring the organisation receiving the information to be bound by the same policies and procedures as the service provider. Service providers facilitate a culture of openness and transparency around how information is handled within the service. Members of staff are encouraged to engage with service users to ensure they understand how their information will be used and answer any questions they may have in this respect.

- Service providers ensure that all new information systems and processes are risk assessed to ensure that they comply with legislation, national standards and evidence-based guidance for information governance. For example a privacy impact assessment (PIA)[¥] is undertaken when proposing to use information for a new purpose and any risks identified are addressed.

2.3.4 Policies and procedures

Safe, good quality care for service users is facilitated by access to and use of good quality data to support decision-making for planning and delivery purposes. Health and social care providers should have effective policies and procedures in place to ensure that they comply with legislation, national standards and best practice guidance on how they gather, record, hold, use and share personal information. These policies and procedures should be available to all staff at a place that is convenient while they are fulfilling their roles. Information governance policies enable all staff working on behalf of a service to implement the service's approach to information governance, while service users can be confident that instances of non-compliance will be dealt with appropriately.

For example

- There are documented policies and procedures to support all aspects of information governance and these are aligned with relevant legislation, standards and evidence-based guidance and are approved at the most senior level within the service. For example policies and procedures should include:

[¥] A PIA is a process designed to identify and address the privacy issues of a particular initiative. It considers the future consequences of a current or proposed action by identifying any potential risks to privacy and then examining ways to mitigate or avoid those risks that have been identified. The Authority has developed a guidance document for completing PIAs which is available at www.hiqa.ie.

- when and how a PIA is undertaken
- procedures for backing up information held electronically that supports contingency and archiving purposes
- an acceptable usage policy governing the use of ICT and personal health information, which all staff are made aware of, for example, the appropriate use of email and faxes
- procedures around 'movers, leavers and joiners', which ensure that access controls are changed as appropriate to reflect a staff member's role within the service as soon as that role changes
- the use of portable devices, including that they are regularly backed-up to the main servers, that they are encrypted and that they should not be left in unattended vehicles or unsecured locations
- procedures to follow should a portable device, for example a mobile phone, be lost
- the secure disposal of files, both paper and electronic
- the appropriate uses and disclosures of information
- obtaining consent
- requirements for passwords to be of a certain standard of complexity, to be changed regularly and that staff are advised of the consequences of the inappropriate use of passwords – including sharing passwords with other members of staff or writing passwords down
- procedures for staff to report security breaches in line with the Data Protection Commissioner's code of practice on data security breaches.

- Policies and procedures for information governance are regularly reviewed and updated, for example, based on the results of risk assessments.
- There is a process for ensuring that policies and procedures and any changes to these are clearly communicated and available to all staff.
- There is a procedure for service users to express concerns about information handling practices. Service users are made aware of this procedure and how to make a complaint.
- There is a procedure for staff to report any risks to information handling practices and for these to become learning opportunities to enable staff members to avoid similar problems in the future.
- There is a statement of information practices for the service outlining how

data may be disclosed in the future for the benefit of the service user, or for purposes not directly related to, or completely separate from the service user's own treatment. The benefits of any proposed secondary uses and their rights in this regard should be clearly explained to service users – for example by outlining the importance of the clinical audit function within a hospital. The statement of information practices is clearly displayed and accessible to all staff and service users.

- Any changes to information handling practices are reflected in the service's statement of information practices in a timely manner.

2.3.5 Training and education

Most members of staff have responsibility for handling personal health information in some capacity. Service users must be confident that staff are sufficiently qualified and trained to fulfil their roles in relation to handling personal information. This is achieved through training and education. Information governance should be a component of induction for new staff and all staff should receive training and education that is tailored to their roles and responsibilities. Refresher training should be provided on an ongoing basis as part of the organisation's training plan. The content of training is regularly reviewed and updated to ensure it is in line with current legislation, national and international standards and evidence-based guidance.

For example

- Information governance is a component of staff induction with repeat training being provided on a regular basis based on changes to systems, policies and procedures and also to continually develop the knowledge and skills of staff.
- Service providers have a training and education programme on information governance that is tailored to roles, responsibilities and levels of access to personal information.
- The training and education programme is evaluated and adapted to reflect changes in legislation, standards, guidance and best available evidence and continues to meet the information governance needs of the service. For example, training and education should include:
  - guidance on coding, disease classifications and data dictionaries where relevant

  - appropriate use of passwords and steps to take in the event of a security breach
  - obtaining consent and how to engage with service users about how their information will be used.
- Staff who are routinely involved in information handling practices are involved in developing the information governance training and education programme so that it reflects actual practice.
- The training material incorporates examples of breaches to information governance policies and procedures that have occurred within the service as well as any risks that have been identified. Actions on how they were dealt with or how they should be dealt with are also included.
- Staff provide feedback on the training programmes and this is reflected in changes to the training material in the future.
- A formal record of training and education attendance is kept to ensure staff competencies are maintained.
- Staff are informed of their responsibility to keep themselves up to date in respect of information governance obligations and requirements.

2.3.6 Self-assessment and continuous improvement

Service users should be confident that the service has a process to regularly assess its compliance with relevant legislation, national standards, evidence-based guidance and its own policies and procedures in order to ensure that information governance practices remain a priority and are regularly reviewed and improved. This facilitates and drives improvements to current practices and ensures that information governance is prioritised. It also enables the service provider to become familiar with and respond quickly to changes in relevant information governance standards and requirements.

Service users are more likely to consent to sharing their personal information for secondary purposes if they are confident that service providers hold their information securely and respect their privacy. This is supported through monitoring, reporting and initiating improvements to information governance practices based on self-assessment.

For example

- Service providers routinely monitor compliance with information governance policies and procedures to identify and act on areas where improvements can be made. The results also inform changes to the information governance training and education programme. Self-assessment includes:
  - monitoring compliance with national standards, guidance or nationally agreed definitions to support sharing and comparison of information
  - evaluating systems and processes used to support data collection to ensure they continue to support the collection of quality data
  - assessing the quality of data, including service users' records and benchmarking performance for quality improvement purposes at a service provider level. This could include auditing an appropriate and random sample of records against reported data to identify if it is accurate valid, reliable, timely, relevant, legible and complete. The sample size should be sufficient to produce reliable measures of data quality
  - auditing and monitoring access to information. For example, the service provider reviews the audit trail* for health and social care records to identify instances of inappropriate access, addition, deletion and editing of information and takes appropriate action based on the results.
- Service providers ensure that regular audits of data collection practices are undertaken to ensure that:
  - the service provider is aware of what information is held, where it is held and how it flows through the service
  - data collection is relevant, evidence-based and aligned with the information needs and requirements of the service.
- Service providers have a data quality assurance programme and institute data quality improvements based on:
  - regular internal data quality audits including the quality of coding that incorporate clinician input
  - external audits and external data quality reports.
- The data on which performance indicators are based is validated by a number of checks, for example, checking data against health and social care records to confirm accuracy of the data.

* An audit trail provides a record of who has accessed electronic records and any changes they have made. Such a record should also be kept of who accesses paper records – for example checking records in and out of the records library.

- Service providers ensure that there is a process to feed back to relevant staff on information governance performance, highlighting identified problems, to facilitate quality improvement and prevent recurrence of errors.
- Service providers engage with service users to assess their satisfaction with how they are being informed about the uses of their information and the ways in which consent is being sought, for example through service user satisfaction surveys.
- Service-user complaints about information-handling practices and the manner in which they are dealt with are reviewed regularly to ensure learning.
- Residual risks from PIAs are reviewed on an ongoing basis to ensure that they are being appropriately managed.

2.4 Data quality

2.4.1 What is data quality?

High quality, safe care relies on access to and use of good quality information. The quality of information available at the point of care contributes to the quality of care delivered to the service user, which in turn impacts on the safety and the effectiveness of services provided, and ultimately on outcomes. High quality information should be the basis on which all decisions regarding health and social care are based, from individual service-user care to national strategic planning. All efforts to improve service-user safety and quality of care are dependent on improvements in access to, and use of, good quality information.

Data quality has been defined as 'the totality of features and characteristics of a data set, that bear on its ability to satisfy the needs that result from the intended use of the data'.[6] Data quality refers to data that is 'fit for purpose' or 'fit for use',[7] and therefore a realistic target for health and social care services is to produce data that is sufficiently accurate, timely and consistent to make appropriate and reliable decisions rather than aiming to produce completely perfect data.[8] Data can be considered to be of good quality when the correct data is available in a timely manner to decision makers who can confidently rely on it.

The quality of data can be determined through assessment against a number of dimensions. Data quality dimensions are 'a set of data quality attributes that represent a single aspect or construct of data quality'.[7] Numerous often overlapping dimensions with different interpretations have been identified in the literature to describe data quality. These dimensions include accuracy, validity, reliability, timeliness, relevance, legibility and completeness, as described in Table 1.

Table 1: Dimensions of data quality

Data quality dimension	What it is	Example
Accurate	It describes or measures what it was designed to describe or measure.	The coding of a clinical record matches the clinical information in the written record.
Valid	It is collected in accordance with any rules or definitions applicable for that information. These rules check for correctness, meaningfulness, and security before the data is processed. This enables comparison and benchmarking over time.	When reporting on the percentage of children in care that have a care plan, only care plans that comply with current child care regulations are reported.
Reliable	It is collected consistently over time, whether manually or electronically.	When reporting waiting time for elective surgery, the same point in time is used by all as the start time, such as the date the patient was placed on the waiting list by the consultant.
Timely	It is collected within a reasonable time period after the activity it measures and it is available when it is required and as often as it is required.	Notifiable diseases are reported to the Health Protection Surveillance Centre in a timely manner to facilitate the identification of an outbreak and the introduction of preventive measures to limit further spread. Accidents and incidents in nursing homes are reported to the person in charge within three days so that trends can be identified.
Relevant	It meets the needs of the information users.	When monitoring uptake of childhood vaccinations it may be necessary to record ethnicity, as future campaigns to improve vaccination uptake may need to be targeted at a particular subgroup of the population.

Legible	It is readable and understandable for the intended users.	A prescription written by a general practitioner (GP) makes clear to the dispensing pharmacist which drug is to be dispensed and in what dosage.
Complete	It has all those items required to describe or measure the intended activity or event.	When a GP refers a service user to a specialist consultant it is important that the referral letter contains all relevant medical details such as the presenting complaint, relevant medical history, findings from physical exam, results of investigations and all prescribed medications.

While each of the dimensions may be considered equally important, there may be instances where the relative importance of one dimension is greater than another. The relative importance of each dimension is based on the requirements of the data user, whether this is for supporting service delivery, quality improvement, performance reporting or planning. For example, to satisfy the timeliness dimension, it may be necessary to sacrifice some element of completeness as by the time the required data is deemed complete it may not be available in a sufficiently timely manner to support decision making.

2.4.2 Why is data quality important?

Quality health and social care is dependent on access to and use of good quality data. Service providers produce a large volume and variety of data. This ranges from administrative data used to manage health and social care services to the numerical values of laboratory results and subjective descriptions of a service user's state of health or wellbeing. This data is collected both electronically and manually in paper-based records, however, data quality is becoming increasingly linked with digital information systems as data is increasingly held in electronic repositories and databases.[9] The quality of all data is important, whether in electronic or manual form, as it contributes to improved outcomes when it can be relied upon to support decision making.

However, according to Statistics Canada,[10] data quality is relative and not absolute and is dependent on financial and human resources; the quality and quantity of data must be balanced against available resources. Recognising that data collection is costly, it is necessary for service providers to ensure that the amount and quality of data collected is aligned with the information needs of the service.

The benefits of good quality data include:

- Service users are more likely to receive safe and effective care if health and social care professionals have access to accurate and reliable data to support decision making. Access to accurate and reliable data such as the results of investigations, allergies, potential drug interactions or past medical history supports healthcare professionals in providing care that is appropriate to assessed needs.
- Service users are more likely to receive safer better care if performance data used to support quality improvement is of good quality and reflects actual performance. Health and social care services institute quality improvement initiatives based on performance measurement.
- Service users will have access to reliable information to inform decisions on where to access care.
- If the data used to support decision making is of a high quality, health and social care services can plan and provide for service-user needs more effectively and efficiently. For example, good quality demographic data that highlights an aging population or a significant increase in immigrants in a specific catchment area can facilitate services in planning for the specific needs of that area.
- Health and social care research contributes to improved outcomes by providing evidence to support particular care processes. This research can only be relied on if it is based on good quality data.

2.4.3 Standards and data quality

Health information standards support data quality by facilitating interoperability[¥] between information systems and through the meaningful and appropriate sharing of data. Standard definitions in the form of data dictionaries, standard terminologies and messaging standards are examples of such standards.

Standard definitions - data dictionary

It is essential to understand precisely what the data means or represents; thus staff need to know consistently, for example, whether the numbers 010573 represents a date of birth or a medical record number based on the standard format of each within their organisation. Typically this description of data – or metadata – is contained in a data dictionary. A data dictionary contains a list of data-element definitions and attributes that support the consistent collection of valid and reliable data and is central to maintaining and improving data quality.

[¥] Interoperability is the ability of health information systems to work together within and across organisational boundaries in order to advance the effective delivery of healthcare for individuals and communities.[11]

According to the American Health Information Management Association[12]

'a data dictionary is a descriptive list of names (also called representations or displays), definitions, and attributes of data elements to be collected in an information system or database. The purpose of the data dictionary is to standardize definitions and therefore have consistency in the collection of data.'

A data dictionary supports the electronic sharing of health information and improves communication by having a shared understanding of data.[12] It facilitates the comparison of activity and performance and the sharing of information across different services and settings.

Standard terminological systems

Terminological systems support data quality by ensuring that the meaning of data is not lost when it is shared between information systems. A terminological system is 'essentially a representation of concepts, attributes and relationships pertaining to medical terms'.[13] Two types of terminological systems are used in healthcare practice: classifications and clinical terminologies.

Classification systems are by far the most widely used approach to code health information. According to the American Health Information Management Association[12] clinical coding:

'is the transformation of narrative descriptions of diseases, injuries, and healthcare procedures into numeric or alphanumeric designations (that is, code numbers). The code numbers are detailed in order to accurately describe the diagnoses (that is, what is wrong with the patient) and the procedures performed to test or correct these diagnoses.'

A clinical coder translates the medical terminology in a healthcare record, such as diagnoses and procedures, into alpha-numeric codes based on a medical classification system, such as International Statistical Classification of Diseases and Related Health Problems – Tenth Revision, (ICD-10). This data is then used for a number of purposes including to report on morbidity and mortality rates and for reimbursement.

Classification systems are used to code diagnoses, procedures or other elements of a healthcare record. For example, the International Statistical Classification of Diseases and Related Health Problems – Tenth Revision, (ICD-10) is widely used to code data for casemix and reimbursement in many countries including the Hospital In-Patient Enquiry System (HIPE)^ in Ireland. However, they are inadequate to support the requirements of documenting clinical care because they are not

^ HIPE is a computer-based system designed to collect demographic, clinical and administrative data on discharges and deaths from acute hospitals nationally. HIPE s managed by the Economic and Social Research Institute (ESRI) in association with the HSE.

sufficiently fine-grained and fail to define all of the individual concepts used within a given healthcare domain.

Clinical terminologies, when compared to classifications, are generally more comprehensive, precise and offer a more accurate representation of the healthcare domain. However, clinical terminologies are not suitable for all applications. For example, they are not suitable for reporting because of their immense size, fine granularity and complex hierarchies, for which, for example, ICD-10 is appropriate.

The full benefits of clinical terminologies are realised when they are used to collect clinical information as part of the clinical encounter and are linked and integrated with classifications to generate data for secondary use, for statistical and epidemiological analysis, external reporting requirements, measuring quality of care and monitoring resource allocation.[14]

Clinical terminologies such as SNOMED CT (Systematized Nomenclature of Medicine – Clinical Terms) are essential to support full semantic interoperability so as to ensure that the information shared/sent can be mutually and unambiguously understood. Increasingly, mappings between terminology and classification systems are being developed so that data can be captured and coded in SNOMED at source as part of the clinical encounter and then aggregated or summarised as appropriate and converted into ICD-10 codes for the purposes of casemix and reporting.

The World Health Organization (WHO) uses the International Classification of Functioning, Disability and Health (ICF) to measure health and disability at both individual and population levels. It is a classification of health and health-related domains classified from body, individual and societal perspectives by means of two lists: a list of body functions and structures, and a list of domains of activity and participation.[15]

In 2001 the ICF was endorsed for use in WHO member states as the international standard to describe and measure health and disability. ICF complements ICD-10, which contains information on diagnosis and health condition but not on functional status.[15]

Messaging standards

Messaging standards outline the structure, content and data requirements of electronic messages to enable the effective and accurate sharing of information.

In the context of messaging standards, the term 'message' refers to a unit of information that is sent from one system to another, such as between a laboratory and a general practitioner (GP).[16]

Specific messaging standards for the healthcare context, such as HL7, are an essential way of improving how we use technology to enable safe and effective information exchange, including the exchange of clinical, administrative and service-user information, for the benefit of the quality and safety of service-user care.

2.4.4 Data quality in practice

Compliance with the guidance provided under the headings of executive level responsibility, accountability, leadership and management, policies and procedures, training and education and self-assessment and continuous improvement outlined in section 2.2 are also required to support a culture of data quality. Additional guidance, specific to data quality, is outlined in this section.

Data collection should be supported by efficient systems and processes that ensure that quality data is available when and where it is needed. Service providers should have systems and processes to support the delivery of safer better care which enable staff to collect and record service-user information accurately on all systems and records. Health and social care records support professionals to provide the best possible care by making care and treatment information available and also facilitate the appropriate sharing of information between health and social care professionals. They include electronic and handwritten notes, demographic data such as name and address, medical history, social history, findings from physical examination, correspondence between health and social care professionals, laboratory reports, specimens, radiological images and reports, clinical photographs and videos, voice recordings and printouts from monitoring equipment.

Service-user information that is inaccessible or inaccurate can lead to the creation of duplicate records, delays in the provision, or compromise the quality and safety, of care. Systems and processes facilitate a consistent means for collecting, analysing, using and sharing information, both manually and electronically, to ensure it is available where and when it is needed.

For example

- Service providers have a robust process to manage the co-existence of paper and electronic records so that there is one authoritative source for up-to-date reliable information.
- Service providers uniquely identify all service users who attend their service and this identifier is used on all service users' records and for communications within and between services.
- Service providers support data collection through the availability of data sets and data dictionaries to enable the consistent collection of data across the service. Data dictionaries should:
  - be freely available and accessible to all staff
  - comply with nationally and internationally agreed definitions where they exist

  - be version controlled and all reports include details of which version was used
  - be updated in a timely manner to incorporate changes to standards and nationally agreed definitions.
- Service providers ensure that data is submitted to regional and national resources in a timely manner, in the required format and that it complies with data definitions.
- To support consistent data collection, data classification or coding manuals should:
  - be easily accessible and readily available to all staff
  - be version controlled and all reports include details of which version was used
- Service-user records are created and maintained using a uniform structure to facilitate the chronological documentation of care and results of investigations to reflect the continuum of care.
- Service-user records are updated in a timely manner to reflect care provision and all entries are legible and attributable.
- Verbal communications about care are documented as soon as is practicable. For example, in emergency situations a doctor may verbally prescribe a particular treatment; this prescription should be recorded in the service user's records as soon as is practicable after the event.
- Paper records are made from robust material and can be secured in place so that there are no loose pages.
- There is a designated place for recording hypersensitivity reactions that is readily identifiable and accessible.
- Data collection should not impact negatively on service-user care and should be integrated into routine activities and business processes so that it is collected as close as possible to the point of care. Data should only be collected and reported once, to reduce the burden of data collection.
- Service providers comply with national standards, guidance or nationally agreed definitions to support sharing and comparison of information.
- Information systems have validation checks to minimise incorrect data entry and to support the collection of complete and valid data. For example, a hospital outpatients department may not issue an appointment with inadequate service-user identification information.

- Service providers comply with national standards, where they exist, that facilitate interoperability of systems and sharing of information.
- Service providers have an accessible log for tracking records that tracks when records are removed from the records department, who removed them, where they are taken and when they were returned. Audit trails should be in place for electronic systems.
- Records retention policies are based on legislation and evidence-based national guidance.
- Records that have been approved for disposal should be destroyed under confidential conditions and in line with environmental health regulations.
- There is a permanent register kept of all classes of records that have been deleted, the time period covered by the records, date of disposal and who was responsible for the disposal.

2.5 Privacy and confidentiality

2.5.1 What are privacy and confidentiality?

In the context of health and social care, privacy can be defined as the right of individuals to prevent information about them from being disclosed and service providers, as data controllers, are obliged to uphold this right. This means that service users have a right to control when, where and with whom, to share their personal health information and these rights are outlined in the Data Protection Acts of 1988 and 2003.[1;2] However, in certain circumstances, access to a service user's personal health information may be granted to other parties under Freedom of Information legislation,[3;4;17] in which case consent may not be required. Such situations might include, for example, access to a child's records by a parent or guardian, access to the records of a deceased person or access to personal records in the public interest.

Confidentiality refers to a duty that a person owes to safeguard information that has been entrusted to him or her by another.[18] In the health and social care context, health and social care providers have a duty of confidentiality to their service users[#] that are founded upon and emphasised both by longstanding ethical duties and legal principles. These are outlined in professional codes of conduct such as the Guide to Professional Conduct and Ethics for Registered Medical Practitioners.[19]

[#] In some cases confidentiality cannot always be guaranteed – for example in the area of child protection and welfare.

Service providers have an obligation to protect personal information provided by service users and not to disclose this information to others without the service user's consent. A duty of confidence arises when one person discloses information to another in circumstances where it is reasonable to expect that the information is held in confidence. For example, it is reasonable for the patient of a GP to expect that information shared in a consultation will be held in confidence.

Health information is considered to be one of the most sensitive forms of information. Health and social care providers collect, use, store and disclose health information in the process of providing safe effective health and social care. This can present a risk to the privacy and confidentiality of service users as increasing amounts of personal health information are processed. Service providers, as data controllers,[+] are obliged to respect the rights of service users in relation to the privacy and confidentiality of their personal health information. Service users' rights to privacy and confidentiality are stated in the Data Protection Acts 1988 and 2003.[1;2] As mentioned in section 2.1.1 of this document, Article 40.3.1º of the Irish Constitution also establishes an implied right to privacy[20] stating that:[21]

> 'The State guarantees in its laws to respect, and, as far as practicable, by its laws to defend and vindicate the personal rights of the citizen.'

2.5.2 Why are privacy and confidentiality important?

Privacy and confidentiality are important because:

- Each individual using health and social care services has specific rights in relation to their privacy as stated in the Data Protection Acts of 1988 and 2003. Service providers have an obligation to uphold these rights and comply with the legislation.
- If service users are confident that their information is being appropriately protected and have trust in the system, then they are more likely to share information, which leads to improved safety and quality of care at an individual level.
- If service users have confidence and trust in service providers they are also more likely to be comfortable with their information being used for secondary purposes, for example, research and service planning, which can yield further benefits to the health of the population and the health and social care system as a whole.

2.5.3 Confidentiality and consent

Service users should be informed of how their personal health information is used. This can be achieved by ensuring that consent is required to use their information for

[+] The Data Protection Commissioner defines a data controller as any individual (e.g. a GP) or organisation/service provider (e.g. a hospital) that collects, uses or discloses personal information. A data controller is the individual or the legal person who, either alone or with others, controls and is responsible for the keeping and use of personal information on computer or in structured manual files.

any purpose other than the delivery of care. Consent is a key component of privacy and confidentiality. It can be defined as a freely given, specific and informed indication of the data subject's wishes to use their personal health information.[22] Consent always has to be informed to be valid. Elements of informed consent around the use of information are:[20]

- Awareness (through the provision of suitable information) and understanding (capacity and competence) of the nature and extent of the processing, especially in terms of the intended and likely uses and disclosures of the information involved.
- Awareness of option(s) to prevent any such processing either in whole or in relation to any particular aspect.
- The existence of a mechanism to enable the option of withholding consent to be effective.
- Absence of coercion.

Typically, consent must be sought in order to use or disclose a service user's personal health information. Whether this consent needs to be implied (inferred by the actions of the service user) or explicit depends on the type of use or disclosure. In either case the consent must be informed and unambiguous. However, there are a number of legislative provisions which confer a responsibility on medical and social care professionals to disclose personal health information – with or without the consent of the person concerned. Examples include the disclosure of notifiable diseases, such as TB, and disclosure of notifiable incidents, such as an allegation of abuse of a nursing home resident.

Further issues arise in instances such as obtaining consent from children, or from their parents on their behalf, or not being able to establish contact with people to obtain their consent. The Freedom of Information Act [Section 28(6)] Regulations 2009[17] and related Guidance Notes,[23] prescribe that records relating to certain classes of individual can be made available to parents and guardians. Records of the deceased may also be made available to certain classes of requester under this legislation. A number of guidelines have been developed around these issues but in case of any doubt advice should be sought from the Office of the Data Protection Commissioner or the Office of the Information Commissioner.

It is important to note that in some cases the risk is greater around not sharing information even without the consent of the individual concerned, such as, for example, in the area of child protection. This is provided for in legislation in the Protection for Persons Reporting Child Abuse Act 1998 which provides immunity from civil liability to any person, acting reasonably and in good faith, who reports (in line with the Act) to designated officers of the HSE or any member of An Garda Síochána his or her opinion that a child has been or is being abused.[20]

2.5.4 Privacy and confidentiality in practice

Compliance with the guidance provided under the headings of executive level responsibility, accountability, leadership and management, policies and procedures, training and education and self-assessment and continuous improvement outlined in section 2.2 is also required to support privacy and confidentiality. Additional guidance, specific to privacy and confidentiality, is outlined in this section.

Service providers should have effective arrangements in place to meet their legal obligations under the Data Protection and Freedom of Information Acts.[1-4] Service users who make a request for personal information should be told if the service holds information about them, what the information is and why it is being held (although if, for instance, the health and mental wellbeing of the service user might be affected by obtaining access to the data, then their access may be limited).

Service users attending a service should be facilitated to access a copy of their personal health and social care records and have factually inaccurate information amended. The service provider's arrangements should ensure that services implement measures to comply with the timescales for responding to an information request. This requires an appropriate records management policy and the identification of members of staff who are accountable for responses to freedom of information requests.

For example

- Service providers have a named individual responsible and accountable for dealing with requests for access to personal information.
- Service providers inform service users of their rights around personal information held about them and the process for accessing their information. This can be done, for example, through leaflets or posters in hospital or GP waiting rooms.
- Service providers inform service users of the reason their information is required and with whom it is shared.
- Service providers enable service users to access a copy of information held about them and correct any factual inaccuracies in their records.

2.6 Information security

2.6.1 What is information security?

Information security, as it applies to health and social care, can be defined as the protection of information from a wide range of threats in order to ensure continuity of care, minimise risk, and maximise the availability of required information in order to provide safe, effective care.[24] In order to be able to use information as a resource for planning, delivering, monitoring, managing and improving care, it must be held securely.

Health information exists in many media and can be required for different purposes. In health and social care, it may be printed or written on paper files, stored electronically, transmitted by post or by using electronic means or messaging, conveyed using television media, or spoken in conversation between health and social care professionals and service users. It is important that health information is appropriately protected in all forms and means by which it is shared or stored. Health information, whether in paper or electronic form, is vital to the provision of safe care to service users and to the business processes of health and social care organisations. Consequently, it is vital that health information is suitably protected. This is especially important in the increasingly interconnected health and social care environment. It is important to recognise the many benefits such interconnectedness can bring, for example extended research possibilities, provided the necessary safeguards are in place. However, as a result of this increasing interconnectivity, information is now exposed to a growing number and a wider variety of threats and vulnerabilities. The safeguards put in place must be appropriate to the level of threat or vulnerability in question.

The Data Protection Acts 1988[1] and 2003[2] place an obligation on data controllers to have appropriate security measures in place to prevent unauthorised access to, or unauthorised amendment, disclosure or destruction of the data. Each member of staff should only be able to access information which they have a justifiable need to access. Audits of information and records accessed by staff should be undertaken to monitor instances of non-compliance. There should be a process in place to audit whether information is being accessed by the appropriate individuals with a genuine need to access it. There must also be processes in place to protect against the accidental loss or destruction of data. Data controllers and data processors are also obliged to ensure that their staff and other persons at the place of work are aware of security measures and comply with them. The legal obligation to keep personal data secure applies to every data controller and data processor, regardless of the size of the service.

Information security can be achieved by implementing appropriate policies, procedures, processes, and organisational structures and functions. This helps to ensure the physical and electronic protection of information whether stored, in use or in transit in such a manner that it is only accessible to those who require access and are fully authorised. Robust information security practices can prevent against

loss, unauthorised amendment or destruction of information. Information security controls should be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the objectives and requirements of health and social care organisations are met.[24] The International Standards Organisation (ISO) has developed two standards[24;25] relating to information security which have been used to inform information security policies in health and social care settings internationally. They are a useful starting point for the development of any information security policy by recommending the actions required in order to assess the type of security controls that are needed.

2.6.2 Why is information security important?

Information security is important because:

- Robust information security arrangements are required in order to ensure the protection of health information and to meet the statutory requirements of the Data Protection Acts 1988 and 2003.[1;2]
- Health information is a valuable resource. Its loss due to theft, system failure or corruption of files could have serious negative consequences for the people to whom the information relates. If appropriate back-up procedures are not in place, the quality of care could be compromised if information is not available when needed.
- Service users need to be confident that their information is held securely and that the appropriate arrangements are in place to prevent the loss of or unauthorised access to that information. The promotion and protection of service users' information is an essential element of person-centred care. Poor information security can lead to data loss which can negatively impact on the reputation of the service for example as a result of media coverage about service user information being stolen or mislaid, leading to service users losing trust in the service.
- Reliable and useful information is required to support the provision and continuity of safe care. Without effective security processes, health information may become unreliable, may not be accessible in the right place at the time it is needed, or may be altered by unauthorised individuals. Unsecured health information cannot be reliably or safely used in the provision of health and social care.

2.6.3 Information security in practice

Compliance with the guidance provided under the headings of executive level responsibility, accountability, leadership and management, policies and procedures, training and education and self-assessment and continuous improvement outlined in section 2.2 is also required to support information security. Additional guidance, specific to information security, is outlined in this section.

Information security should be supported by efficient, effective and up-to-date systems and processes to ensure information is held securely from current and emerging threats. These systems and processes should encompass threats to both the physical and electronic security of information and protect against loss, corruption, destruction, unauthorised access, alteration or deletion of personal health information, whether held in paper or electronic form. Service providers should have systems and processes in place to prevent each of these occurring but also mechanisms in place to deal with the consequences should such an event occur and to recover from it in the least amount of time possible with the least possible impact on service users, staff and the service as a whole.

For example

- Paper and electronic files are stored securely when not in use.
- Buildings and areas where records are stored are physically secure from unauthorised access, fire and flood damage.
- There is a mechanism in place to ensure that all data stored on equipment or devices that have been made redundant or are to be re-used are fully erased.
- All staff members who have access to electronic records have individual login details and passwords.
- Access to areas where records are stored, data centres and server rooms used to host hardware and software on which personal data is stored are restricted to only those staff members that have clearance to work there, for example through the use of swipe card access.
- Information systems are risk assessed to ensure that they remain fit for purpose and the results of assessments are acted on appropriately.
- Information systems have anti-virus software installed that is kept up to date and protects from all sources of possible infection, including the Internet and removable storage devices, such as USB keys.
- All portable devices that are capable of handling or displaying personal health information and databases are password protected and encrypted.
- Staff-owned devices such as portable media players, digital cameras and USB keys are technologically restricted from connecting to the service's computers or network.

- There are technologies in place that allow for the remote deletion of information from portable devices, such as mobile phones, if such devices are lost or stolen.
- The service ensures that its ICT systems are protected by the use of appropriate firewall technologies and that this technology is kept up to date and is sufficient to meet emerging threats.
- External service providers, and individuals or agencies undertaking work on behalf of the service are subject to strict procedures with regard to access to information and areas where information is stored, by way of formal contract.
- There is a disaster recovery plan in place that is regularly reviewed to ensure that it is fit for purpose. Recovery arrangements are tested regularly and the results are reported to senior management.

2.7 Secondary use of information

2.7.1 What is the secondary use of information?

As a general rule, information should only be used for the primary purpose for which it was collected. Primary purpose relates to information which has been collected and is being kept by a custodian for the purpose of protecting, promoting, maintaining or meeting the physical and mental health needs of an individual.[20] Secondary use of information relates to information collected in the course of providing care, being used for purposes other than direct service-user care. Service-user data can be used for many valuable secondary purposes, which bring benefits to the service-user population as a whole.

Each proposed secondary use of information will vary according to circumstances. Therefore, service providers must risk assess the uses and exercise their judgment to determine what steps to take, assess the privacy risks and what safeguards to put in place.

Information is a valuable resource and as such, wherever possible, it should be collected once and used many times – provided the appropriate protections and safeguards are in place. There is a need to strike a balance between people's right to personal data privacy and the desirability of making information available to improve the quality and effectiveness of care through audit and research for the public good.

The key concept in respect of the secondary use of information is informing service users so that there is a shared expectation of how their personal information will be used and obtaining consent where it is necessary. There are a number of exceptions to this, which are provided for in legislation. For example, the Health (Provision of

Information) Act 1997 allows for the provision of information to the National Cancer Registry without the consent of the service users concerned. Medical professionals also have a legal obligation to disclose details of notifiable diseases with or without consent, as set out in Infectious Diseases Regulations. Except for where there are legislative provisions to the contrary, service users should be in control of how their information is used and consent must be sought for proposed secondary uses.

Personal information ceases to be 'personal' only when it has been anonymised to the point that it can no longer be linked to a known individual, meaning the removal of all possible identifying details and ensuring that any other data or combination of data could not identify the individual.[22] However, it is difficult to fully anonymise data as typically there is some link back to the individual or a mechanism to reverse any coding that has taken place.

Once information has been irrevocably anonymised, the provisions of the Data Protection Acts no longer apply. It is not necessary to obtain consent to use anonymised data for secondary purposes but best available evidence suggests that service users should still be informed. This can be achieved through including the possibility of use of anonymised information for secondary purposes in the organisation's statement of information practices. An overview of what should be contained in a statement of information practices is outlined in Appendix 1.

The Authority is concerned with ensuring the appropriate safeguards are in place to protect service users' rights to privacy and confidentiality of their personal health information. As such in the context of this document the term secondary use of information can be taken to mean the secondary use of personal health information.

Secondary uses include using information for:

- Audit and quality assurance purposes – for example using individuals' health and social care records to complete audits to support continuous improvement in the delivery of care.
- Performance monitoring – for example the Health Service Executive (HSE) uses HealthStat[±] to measure waiting times for services in public hospitals throughout the country, to assess if targets are being met and to identify areas where improvements are required.
- Planning of services – for example Hospital In-Patient Enquiry (HIPE)[»] data are used by the Department of Health and the HSE in the planning, provision and measurement of acute hospital services and also for the allocation of resources.

[±]HealthStat is a performance information and improvement system designed and implemented by the HSE. It is a databank of performance information for Irish public health services.

[»]HIPE is a computer-based system designed to collect demographic, clinical and administrative data on discharges and deaths from acute hospitals nationally. HIPE is managed by the Economic and Social Research Institute (ESRI) in association with the HSE.

- Research on the incidence, prevalence and causes of conditions – for example information collected by the National Cancer Registry – can be studied to determine patterns in distribution and determinants of the incidence of cancer cases. Although the National Cancer Registry has a legislative remit to collect this information, as set out in the Health (Provision of Information) Act 1997, this is secondary use of the information as it was primarily collected at the point of care for the purpose of providing treatment to the service user.
- Research conducted within a hospital aimed at improving service-user outcomes, for example the impact of Vitamin D supplementation in the reduction of falls among service users with a history of osteoporosis fractures.

As can be seen from the examples documented above there are varying levels of secondary use of information, some of which can be conducted using pseudonymised data, which carries little or no risk of individual identification. Pseudonymisation involves the use of a coding system to protect the identity of an individual to whom the information relates. Pseudonymous records are distinguishable but cannot be associated with a specific person. Information should be pseudonymised at the earliest possible stage of the secondary use, thereby minimising the risk to the service users' privacy.

While safeguards are still required they may not be as stringent as those necessary when proposing to use identifiable service user data. In some instances, such as planning of services, consent inferred by the actions of the service user may be sufficient. However, the consent must be informed. In the case of research it may be necessary first to seek approval from a research ethics committee and to comply with its requirements.

2.7.2 Why are safeguards around the secondary use of information important?

Being able to use information for secondary purposes is necessary in order to quality assure the care that is being provided, for example, through clinical audit. It is a requirement of the *National Standards for Safer Better Healthcare*[26] that service providers use information as a resource in planning, delivering, managing and improving the quality, safety and reliability of healthcare.

The secondary use of information can lead to more informed decision making, higher quality and safer care for everyone and better use of public monies benefiting all users of health and social care services.

However, service users need to be aware of these secondary uses and be comfortable with how and why their information is being used. Safeguards around the secondary use of information are important because:

- Informing service users of the benefits of such secondary uses and that their information may be used in this way increases their confidence and trust in the service.

- Service users need to be confident that their rights are being appropriately protected and respected and ultimately know that they are in control of how their information is being used.

2.7.3 Secondary use of information in practice

Compliance with the guidance provided under the headings of executive level responsibility, accountability, leadership and management, policies and procedures, training and education and self-assessment and continuous improvement outlined in section 2.2 is also required to support the appropriate secondary use of information.

Additional guidance, specific to the secondary use of information is outlined in this section, which focuses on person-centred care and informing service users.

Consent is a key concept in the context of the secondary use of information. At the most basic level of interpretation, consent must be obtained for the collection, use or disclosure of information for purposes outside the direct provision of care. However, there are exceptions to this – based on the type of secondary use explicit consent may be required or consent implied by the actions of the service user may be sufficient. The requirement for explicit or implied consent is generally proportionate to the level of risk to the service user and how closely the use is related to the provision of care. For example where local clinical audit may be carried out in a hospital it will be sufficient to inform service users through a statement of information practices or leaflets or posters in a waiting room.

However, when proposing to use information for research, explicit consent must be sought and approval may be required from a research ethics committee. In many cases it is possible to use anonymised information for research purposes meaning that it would not be necessary to obtain consent but best practice indicates that service users should still be informed, which as previously indicated, can be achieved through the service provider's statement of information practices.

Explicit consent is consent that is clearly and unmistakably stated. It may be obtained in writing, orally, or in any other form where the consent is clearly communicated. Where such consent is required, it should always be recorded, dated and preferably signed and witnessed.[20]

In some cases consent can be inferred by the actions of the service user. For example, by presenting for treatment at a GP practice a service user is implying their consent to be treated, and by agreeing to a referral to a specialist is consenting to their information being shared for this purpose. However, service users still need to be informed of how their information will be used. Both explicit and implied consent must be informed to be valid. If at a later stage questions are raised about uses of information the burden of proof falls to the service provider to demonstrate that the consent was informed and unambiguous.

Service providers should be open and transparent with service users about the various uses of their information. This can be done verbally and through clearly displayed information leaflets or statements of information practices outlining the ways in which information may be used, the reasons for it and the associated benefits, such as improvements in service delivery.

For example

- Staff obtain consent where necessary and are aware of the procedures that must be followed in this regard and in informing the service user as to how their information will be used.
- Information is provided to service users in a manner which they can understand, for example, if English is not their first language or if they have literacy problems.
- Staff answer any questions people may have in relation to the use of their information or arrange for them to speak with someone in a position to discuss any concerns they may have.
- Service users are informed of the benefits of their information being used for secondary purposes.
- Service users are assured that their refusal to give consent to the use of their information for a secondary purpose will not adversely affect the care they receive from the service.

3. Legal obligations around information governance

3.1 Introduction

In Ireland, there is general and health-specific legislation, which impact on the handling and management of information. Pending the publication and enactment of the Health Information Bill, the most relevant legislation for the handling and management of information in health and social care is the Data Protection Acts and the Freedom of Information Acts.[1-4] There are a number of other acts containing specific provisions relating to the management of information that also warrant consideration.

It is the duty of service providers to ensure that they are aware of and comply with all relevant legislation. A process should be in place to ensure that they are made aware of the enactment, modification or repeal of legislation that pertains to them. This section documents some of the legislation relevant to information governance, under the following headings:

- the Constitution
- national legislation.

3.1.1 The Constitution

Although there is no express reference to a right to privacy in the Irish Constitution, the Supreme Court has ruled that an individual may invoke the personal rights provision in Article 40.3.1º which establish an implied right to privacy.[20] Specifically, Article 40.3.1º states:[21]

'The State guarantees in its laws to respect, and, as far as practicable, by its laws to defend and vindicate the personal rights of the citizen.'

3.1.2 National legislation

National legislation makes provision for information governance. The following list highlights a number of the main pieces of legislation relating to information governance:

- The forthcoming Health Information Act
- Data Protection Acts 1988 and 2003, and associated regulations
- Data Protection (Access Modification) (Health) Regulations 1989
- Freedom of Information Acts 1997 and 2003, and associated regulations
- The Health (Provision of Information) Act 1997
- The Statistics Act 1993

- Infectious Diseases Regulations 1981, Infectious Diseases (Amendment) (No. 3) Regulations 2003 and Infectious Diseases (Amendment) Regulations 2011.

The Health Information Act

At the time of writing this guidance document, the Health Information Bill is being drafted. One of the main objectives of the Health Information Bill is to underpin an effective information governance structure for the health system generally, building on legislation that is already in place and working well, namely data protection and freedom of information legislation. It is anticipated that the Bill will be published in 2013.

The Data Protection Acts 1988 and 2003

In 1988, the Data Protection Act[1] was passed in order to implement the 1981 *Council of Europe Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data*.[27] The Act regulates the collection, processing, keeping, use and disclosure of computerised personal information relating to living identifiable individuals. It covers both the private and public sectors. The Data Protection Act of 2003 strengthened individuals' rights (as data subjects) in relation to their personal information and imposed more obligations on those who keep such information (data controllers). The Data Protection Act of 2003 also extends data protection law to manual records and introduces special provisions in relation to categories of sensitive information, including personal health information.[28]

The Data Protection Commissioner (the Commissioner, hereafter) has statutory responsibility for implementing the terms of the Data Protection Acts and has a wide range of powers which can legally oblige a person holding personal data to comply with the terms of the Acts. These powers include the requirement for a person to provide information needed to assist with enquiries being carried out by the Office of the Data Protection Commission and restrict the transfer of information abroad. The Commissioner is responsible for upholding the rights of individuals as set out in the Acts, and enforcing the obligations upon data controllers. The Commissioner is appointed by the Government and is independent in the exercise of his or her functions. Individuals, who believe that their rights in relation to their personal data are being infringed, can complain to the Commissioner, who will investigate the matter, and take whatever steps may be necessary to resolve the matter.

One of the core functions of the Office of the Data Protection Commissioner is to enforce the data protection legislation. The Office of the Data Protection Commissioner has been conducting compliance audits, including audits of healthcare facilities, against data protection legislation since 2003. A compliance audit typically examines a service's procedures, policies, systems and records in order to assess whether the service is generally in compliance with the provisions of data protection legislation.

The eight principles of Data Protection as outlined in the Act dictate that data controllers must:

- obtain and process information fairly
- keep it for one or more specified, explicit and lawful purposes
- use and disclose it only in ways compatible with these purposes
- keep it safe and secure
- keep it accurate, complete and up-to-date
- ensure that it is adequate, relevant and not excessive
- retain it for no longer than is necessary for the purpose or purposes
- give a copy of his/her personal data to an individual, on request.

These principles, when applied in the health and social care setting relate to:

- using, disclosing and transferring personal health information
- service-user consent to collecting information
- service-user access to personal health information.

Data Protection (Access Modification) (Health) Regulations 1989

These regulations prohibit the supply of health data to a service user in response to a request for access in the case that such access would cause serious harm to his or her physical or mental health. The legislation also makes the provision that such data is to be communicated only by, or after consultation with, an appropriate 'health professional' — normally the service user's own doctor.[29]

The Freedom of Information Acts 1997 and 2003

The Freedom of Information Act 1997,[3] as amended by the Freedom of Information Act 2003,[4] grants individuals the legal rights to access both personal and non-personal information and to have their personal information amended if it is inaccurate. The Office of the Information Commissioner has been established to review decisions by, and practices of, public bodies in addition to the operation of the Acts.[30]

The Freedom of Information Acts 1997 and 2003 apply to public bodies and give individuals the legal right to:[18]

- access both personal and non-personal (organisational and corporate) records
- have personal records amended or deleted where the information is incorrect, incomplete or misleading
- seek reasons for decisions that affect them.

Freedom of Information (FOI) legislation does not apply to the private sector and therefore, private hospitals and general practitioner (GP) practices are not covered by the relevant Acts. However, where a private entity is providing services to the public sector, for example, GPs providing services to medical card holders, then FOI legislation applies.

Health (Provision of Information) Act 1997

The National Cancer Registry in Ireland is in a unique position in that specific legislation allows for this function in the form of the Health (Provision of Information) Act 1997. The Act allows for the provision of information to the National Cancer Registry Board.

The Act also allows the 'the Minister for Health or a Health Board, hospital or other body or agency participating in any cancer screening' to request information from data controllers or data processors as defined in the Data Protection Act, 1998.

The Data Protection Commissioner (in his Annual Report for 1997)[29] stated that the Health (Provision of Information) Act:

> '…identifies an overriding public interest – cancer prevention – and enables an exchange of personal data between data controllers which would not otherwise be permissible.'

In the absence of such specific legislation, where it is necessary for the information used to be identifiable for linking or tracking purposes, the processing of the information must be undertaken with the consent of the individual involved and with the appropriate safeguards to protect their privacy and identity.

Statistics Act, 1993

The Statistics Act, 1993[31] officially established the Central Statistics Office (CSO). Under the Act, the CSO is permitted to collect personal information. For example, the CSO collects and registers information about births and deaths of individuals. It also collects information on health and social conditions, for example generating statistics on acute hospital services and on disability, carers and voluntary activities.

Health Act 1947 and Infectious Diseases (Amendment) Regulations 2011

The Health Act 1947[32] introduced statutory notification of infectious diseases in Ireland. Under the Act, healthcare professionals have a legal obligation to report certain notifiable diseases including tuberculosis (TB), human immunodeficiency virus (HIV) and acute anterior poliomyelitis (Polio) as detailed in the Infectious Diseases (Maintenance) Regulations 1981[33] These regulations have been amended on a number of occasions, most recently in 2011.[34]

3.2 Developments in Europe

At the time of writing, the European Commission has proposed a comprehensive reform of the EU's 1995 data protection rules. The Commission has noted that the 27 EU member states have implemented the 1995 rules differently, which has led to divergences in enforcement.[35] If adopted, the reforms will eliminate this fragmentation and promote consistency across the EU. The proposals to modernise the 1995 Data Protection Directive, on which current data protection legislation in Ireland is based, include a policy setting out the Commission's general objectives and two legislative proposals:

- a regulation setting out a general EU framework for data protection
- a directive on protecting personal data processed for the purposes of prevention, detection, investigation or prosecution of criminal offences and related judicial activities.[35]

4. National Standards

It is recognised internationally that the setting of standards and the monitoring of compliance with them are important levers in driving improvements in quality and safety in health and social care.[36] By incorporating national and international best available evidence, standards assist in promoting health and social care that are up to date, consistent and responsive to the needs of the people who use them. Importantly, standards set out how providers should organise, deliver and improve services and thus enable them to be accountable to service users and funding agencies.

Standards give a shared voice to the expectations of the public, of services users and of service providers. They create a basis for improving the quality and safety of services by identifying strengths and highlighting areas for improvement. While standards frequently form part of a regulatory framework, they are also created to be used in day-to-day practice to encourage a consistent level of quality and safety in health and social care services.

4.1 The Authority and national standards

The Authority has a statutory role under the Health Act 2007 to set standards and to monitor compliance with them to support and promote the provision of safe and effective health and social care services (see Appendix 2). Health and social care services include:

- health care services (excluding mental health) provided or funded by the Health Service Executive (HSE) including, but not limited to including hospital care, ambulance services, community care, primary care and general practice
- residential services for older people
- residential services for people with disabilities (children and adults)
- special care units for children
- children's community residential units
- HSE services for the protection and welfare of children
- foster care services.

4.1.1 Development of standards

To inform the development of standards, the Authority reviews how other countries describe quality in health and social care, looks at the experience of setting standards in other countries, examines national reports and reviews of quality and safety in Ireland, considers the views of service users and the public, and uses experience from its own activities in monitoring, inspecting and investigating services in Ireland.

The Authority works with advisory groups to develop standards and consults widely on draft standards before finalising them and submitting them to the Minister for Health and/or Minister for Children and Youth Affairs for approval and mandating.

As quality in health and social care is multifaceted the trend internationally is to describe care quality according to quality dimensions. The dimensions of a quality service and the capability and capacity factors required to deliver a quality and safe service are reflected in a number of themes. These themes are captured in the Authority's framework for developing standards. The themes described in the *National Standards for Safer Better Healthcare*,[26] and typically used in developing other standards, are:

- **Person-centred care and support** – how services place the service user at the centre of their delivery of care. This includes the concepts of access, autonomy, equity and protection of rights.
- **Effective care and support** – how services deliver best achievable outcomes for service users and meet the needs of service users in the context of that service, reflecting best available evidence and information. This includes the concepts of service design and sustainability.
- **Safe care and support** – how services avoid, prevent and minimise harm to service users and learn from when things go wrong.
- **Better health and wellbeing** – how services identify and take opportunities to support service users in increasing their independence, and their control over improving their own health and wellbeing.

Delivering improvements in the quality of services is dependent on key capacity and capability factors including:

- **Governance, leadership and management** – the arrangements put in place by a service for accountability, decision making, risk management as well as meeting their strategic, statutory and financial obligations.
- **Use of information** – actively using information as a resource for planning, delivering, monitoring, managing and improving care.
- **Workforce** – planning, recruiting, managing and organising a workforce with the necessary numbers, skills and competencies.
- **Use of resources** – using resources effectively and efficiently to deliver best achievable outcome for service users for the money and resources used.

The Authority developed this guidance on information governance under the Use of Information theme from the National Standards following a review of national and international practice in relation to information governance in health and social care services (see the methodology used in Appendix 3).

4.2 Use of Information

The standards set by the Authority recognise the importance of the use of information and facilitate organisations to ensure that:

- the appropriate management and workforce structures are in place to oversee information governance arrangements
- information is used ethically in a manner that protects the rights and best interests of service users
- information within computerised and paper-based systems is held securely and is accurate and available when and where needed (for example, in the event of an unplanned attendance/admission)
- processes and procedures for information and records management are efficient and effective
- staff are provided with guidance and appropriate, effective training
- information is shared appropriately to facilitate the safe transfer and sharing of care.

In services that meet standards set by the Authority, information is:

- held securely and confidentially
- obtained fairly and efficiently
- recorded accurately and reliably
- used effectively and ethically
- shared appropriately and lawfully.

As well as being explicitly stated in some of the national standards, good information governance and information use is essential for services to meet all national standards for quality and safety.

Quality information is an important resource for service providers in planning, managing, delivering and monitoring the quality and safety of services they provide (see Appendix 2). Using information from and about service users is essential in providing a service that responds to their needs. Access to quality information supports evidence-based decision making and facilitates the optimal use of resources to provide efficient and effective care. Consulting with service users and providing them with information regarding their care and/or treatment options and the services available promotes their participation in making informed decisions about their own care.

The aim of this document is to provide more detailed guidance for information governance to support health and social care providers become compliant with the information governance requirements of the National Standards and by so doing implement good information governance practices so that personal information is managed securely, efficiently, effectively and in line with legislation. Further resources to assist healthcare providers are listed in Appendix 4 of this guidance.

References

(1) The Data Protection Act. 1988. Available online from: http://www.irishstatutebook.ie.

(2) The Data Protection (Amendment) Act. 2003. Available online from: http://www.dataprotection.ie.

(3) The Freedom of Information Act. 1997. Available online from: http://www.irishstatutebook.ie.

(4) The Freedom of Information (Amendment) Act. 2003. Available online from: http://www.oireachtas.ie.

(5) NHS Connecting for Health. *Information Governance Toolkit - Derivations and Support for Standards.* 2007. Available online from: http://www.connectingforhealth.nhs.uk.

(6) Arts DGT, de Keizer NF, Scheffer G-J. Defining and Improving Data Quality in Medical Registries: A Literature Review, Case Study, and Generic Framework. *Journal of the American Medical Informatics Association.* 2002; 9(6): pp.600-11.

(7) Wang RY, Strong Diane M. Beyond Accuracy: What Data Quality Means to Data Consumers. *Journal of Management Information Systems.* 1996; 12(4): pp.5-34.

(8) Kerr K, Norris T, Stockdale R. *Data Quality Information and Decision Making: A Healthcare Case Study.* In: *18th Australasian Conference on Information Systems.* 2007.

(9) Kerr K. *The Institutionalisation of Data Quality in the New Zealand Health Sector.* [PhD]. University of Auckland; 2006. Available online at: http://researchspace.auckland.ac.nz.

(10) Statistics Canada. Statistics Canada: *Quality Guidelines.* 2009. Available online from: http://www.statcan.gc.ca/start-debut-eng.html.

(11) Health Information and Management Systems Society (HIMSS). *Interoperability definition and background* [Online]. Available from: http://www.himss.org/content/files/interoperability_definition_background_060905.pdf. Accessed on: 15 September 2011.

(12) American Health Information Management Association. *American Health Information Management Association* [Online]. Available from: http://ahima.org/Default.aspx. Accessed on: 13 December 2011.

(13) Fieschi M et al. Fieschi M et al., (Ed.). *The Specification of a Frame-based Medical Terminological System in Protégé.* In: *Proceedings of the 11th World Congress on Medical Informatics.* 1 January 2004. 2004.

(14) Alberta Health and Wellness. *Adopting and Implementing Clinical Vocabularies: Business Impact Analysis Report.* 2007. Available online from: http://www.nihi.ca/. Accessed on: 28 October 2011.

(15) World Health Organization. *International Classification of Functioning, Disability and Health (ICF)* [Online]. Available from: http://www.who.int/classifications/icf/en/. Accessed on: 2 April 2012.

(16) Health Information and Quality Authority. *General Practice Messaging Standard Version 2.0.* 2011. Available online from: www.hiqa.ie.

(17) S.I. No. 387/2009 - Freedom of Information Act (Section 28(6)) Regulations. 2009.

(18) The Department of Health and Children. *Discussion Document on Proposed Health Information Bill.* 2008. Available online from: http://www.dohc.ie.

(19) The Medical Council. *Guide to Professional Conduct and Ethics for Registered Medical Practitioners.* 2009. Available online from: http://www.medicalcouncil.ie.

(20) The Department of Health and Children. *Draft Heads of Health Information Bill.* 2009.

(21) Bunreacht na hEireann. 1937. Available online from: http://www.taoiseach.gov.ie.

(22) The Office of the Data Protection Commissioner. *Data Protection Guidelines on Research in the Health Sector.* 2007. Available online from: http://www.dataprotection.ie.

(23) Freedom of Information Central Policy Unit. *Guidance Notes on Access to records by parents/guardians, Access to records relating to deceased persons under section 28(6) of the Freedom of Information Act 1997.* 2009.

(24) International Standards Organisation. *Information technology-Security techniques-Code of practice for information security management.* ISO/IEC FDIS 17799:2005 (E). 2005.

(25) International Standards Organisation. *Information Technology – Security techniques – Information Security Management Systems – Requirements.* ISO/IEC 27001:2005(E). 2005.

(26) The Health Information and Quality Authority. *National Standards for Safer Better Healthcare.* 2012.

(27) The Council of Europe. *Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data* [Online]. Available from: http://conventions.coe.int.

(28) The Office of the Data Protection Commissioner. *Data Protection (Amendment) Act 2003 - A Summary Guide.* 2003. Available online from: http://www.post.trust.ie.

(29) Data Protection (Access Modification) (Health) Regulations. 1989. Available online from: http://www.irishstatutebook.ie.

(30) FOI Central Policy Unit, The Department of Finance. *A Short Guide to the*

Freedom of Information Act 1997 and Freedom of Information (Amendment) Act 2003. 2004. Available online from: http://www.foi.gov.ie.

(31) The Statistics Act. 1993. Available online from: http://www.irishstatutebook.ie.

(32) The Health Act. 1947. Available online from: www.irishstatutebook.ie.

(33) Infectious Diseases (Maintenance) Regulations . 1981. Available online from: http://www.irishstatutebook.ie.

(34) Infectious Diseases (Amendment) Regulations . 2011. Available online from: www.irishstatutebook.ie.

(35) The European Commission. *Commission proposes a comprehensive reform of the data protection rules* [Online]. Available from: http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm. Accessed on: 2 February 2012.

(36) The Commission on Patient Safety and Quality Assurance. *Building a Culture of Patient Safety.* 2008.

(37) Social Care Programme. *Social Studies* [Online]. Available from: www.socialstudies.ie. Accessed on: 14 December 2011.

(38) The Department of Health and Children. *The National Health Information Strategy.* 2004. Available online from: http://www.dohc.ie.

(39) The Department of Health and Children. *Quality and Fairness: A Health System for You.* 2001. Available online from: http://www.dohc.ie/publications/quality_and_fairness.html.

(40) The Department of Health and Children. *Proposed Health Information Bill.* 2009. Available online from: http://www.dohc.ie.

(41) The Health Act 2007. Dublin: The Stationery Office; 2007. Available online from: http://www.irishstatutebook.ie/2007/en/act/pub/0023/index.html.

(42) The Health Information and Quality Authority. *What you should know about Information Governance: A Guide for health and social care staff.* 2011. Available online from: http://www.hiqa.ie/.

(43) The Health Information and Quality Authority. *Information Governance Self-Assessment Tool.* 2011. Available online from: http://www.hiqa.ie/.

(44) The Health Information and Quality Authority. *An "As Is" Analysis of Information Governance in Health and Social Care Settings in Ireland.* 2010. Available online from: http://www.hiqa.ie.

(45) The Health Information and Quality Authority. *International Review of Information Governance Structures.* 2009. Available online from: http://www.hiqa.ie.

(46) The Health Information and Quality Authority. *International Review of Health Information Governance Management.* 2011. Available online from: www.hiqa.ie.

(47) The Health Information and Quality Authority. *International Review of Data Quality.* 2011. Available online from: www.hiqa.ie.

(48) The Health Information and Quality Authority. *Guidance on Privacy Impact Assessment in Health and Social Care.* 2010. Available online from: www.hiqa.ie.

(49) The Health Information and Quality Authority. *International Review of Information Security.* 2012. Available online from: www.hiqa.ie.

(50) The Health Information and Quality Authority. *International Review of Secondary Use of Personal Health Information.* 2012. Available online from: www.hiqa.ie.

Glossary of terms

Accountability: being answerable to another person or organisation for decisions, behaviour and any consequences.

Audit: the assessment of performance against any standards and criteria (clinical and non-clinical) in a health or social care service.

Benchmarking: a continuous process of measuring and comparing care and services with similar service providers.

Clinical audit: a quality improvement process that seeks to improve service-user care and outcomes through systematic review of care against explicit criteria and the implementation of change.

Clinical governance: a system through which service providers are accountable for continuously improving the quality of their clinical practice and safeguarding high standards of care by creating an environment in which excellence in clinical care will flourish.

Confidentiality: the right of individuals to keep information about themselves from being disclosed.

Corporate governance: the organisational framework that incorporates systems, processes and behaviours which support the workforce to do the right thing or make the right decision at the right time and demonstrate the provision, management or evaluation of a quality service.

Culture: the shared attitudes, beliefs and values that define a group or groups of people and shape and influence perceptions and behaviours.

Data: data are numbers, symbols, words, images graphics that have yet to be organised or analysed.

Data controller: a data controller is the individual or the legal person who, either alone or with others, controls and is responsible for the keeping and use of personal information on computer or in structured manual files.

Data processor: a data processor processes personal data, but does not exercise control over the personal data. Their responsibilities instead concern the necessity to keep personal data secure from unauthorised access, disclosure, destruction or accidental loss. A data processor is legally distinct from the data controller for whom they are processing the personal data. Someone who is not employed by the data controller, but is contracted to provide a particular data processing service on behalf of a data controller (such as a payroll company) would be a data processor.

Data quality: data that is accurate, valid, reliable, relevant, legible, complete and available in a timely manner.

Effective: a measure of the extent to which a specific intervention, procedure, treatment, or service, when delivered, does what it is intended to do for a specified population.

Efficient: use of resources to achieve optimal results with minimal waste.

Evaluation: a formal process to determine the extent to which the planned or desired outcomes of an intervention are achieved.

Evidence-based: the practice of consistently using current best available evidence in making decisions.

Governance: in healthcare, an integration of corporate and clinical governance; the systems, processes and behaviours by which services lead, direct and control their functions in order to achieve their objectives, including the quality and safety of services for service users. See also Clinical governance and Corporate governance above.

Health: the state of complete physical, mental and social wellbeing and not merely the absence of disease or infirmity.

Health information technical standards: standards that support interoperability between systems and meaningful sharing of data.

Healthcare: services received by individuals or communities to promote, maintain, monitor or restore health.

Health or social care professional: a person who exercises skill or judgment relating to any of the following activities:

a) the preservation or improvement of the health or wellbeing of others

b) the diagnosis, treatment or care of those who are injured, sick, disabled or infirm

c) the resolution through guidance, counselling or otherwise of personal, social or psychological problems

d) the care of those in need of protection, guidance or support.

Health/social care record: all information in both paper and electronic formats relating to the care of a service user.

Induction: the process of preparing new employees for their role.

Information: information is data that has been processed or analysed to produce something useful.

Information governance: the arrangements that service providers have in place to manage information to support their immediate and future regulatory, legal, risk, environmental and operational requirements.

Information security: relates to having systems in place to ensure that all information is held confidentially and securely, can be relied upon in use, and is available to authorised persons when and where needed.(5) It is concerned not only with technical methods for securing information but also deals with physical security measures.

Informed consent: voluntary authorisation by a service user with full comprehension of the risks and benefits involved for any medical treatment or intervention, provision of personal care, participation in research projects and provision of the service user's personalised information to a third party.

Interoperability: the ability of health information systems to work together within and across organisational boundaries in order to advance the effective delivery of healthcare for individuals and communities.[11]

Key performance indicator (KPI): specific and measurable elements of practice that can be used to assess quality and safety of care.

Leadership: leadership involves influencing and organising a group of people to achieve a common goal.

Monitoring: systematic process of gathering information and tracking change over time. Monitoring provides a verification of progress towards achievement of objectives and goals.

Personal health information: personal information is data relating to an individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller.[1] The term personal health information is broad and includes such matters as personal information relating to the physical or mental health of the individual, as well as any genetic data or human tissue data that could be predictive of the health of the individual or his or her relatives or descendants. In essence it covers any information relating to an individual that is collected for or in connection with the provision of a health service.

Policy: a written operational statement of intent which helps staff to make appropriate decisions and take actions, consistent with the aims of the service provider, and in the best interests of service users.

Primary care: an approach to care that includes a range of services designed to keep people well. These services range from promotion of health and screening for disease, to assessment, diagnosis, treatment and rehabilitation as well as personal social services.

Privacy: privacy can be defined as the right of individuals to keep information about them from being disclosed.

Procedure: a procedure is a specification of series of actions, acts or operations which have to be executed in the same manner in order to always obtain the same result in the same circumstances.

Process: a series of steps or actions taken to achieve an end.

Quality information: data that has been processed or analysed to produce something useful and is accurate, valid, reliable, timely, relevant, legible and complete.

Risk: the likelihood of an adverse event or outcome.

Risk management: the systematic identification, evaluation and management of risk. It is a continuous process with the aim of reducing risk to an organisation and individuals.

Secondary use of information: secondary use of information relates to information collected in the course of providing care, being used for purposes other than direct service user care such as audit, performance reporting, service planning and research.

Service provider: any person, organisation, or part of an organisation delivering healthcare services – as described in the Health Act 2007 Section 8(1)(b)(i)–(ii).

Service user: the term service user includes: people who use health and social care services; parents, guardians, carers and family and potential users of health and social care services.

Service: anywhere health or social care is provided. Examples include but are not limited to: acute hospitals, community hospitals, district hospitals, health centres, dental clinics, GP surgeries, home care, etc.

Social care: social care involves the provision of care, protection, support, welfare and advocacy for vulnerable or dependent clients, individually or in groups.[37]

Standard: a statement which describes the high-level outcome required to contribute to quality and safety.

Statement of information practices: a statement of information practices is a document, made available to service users, that sets out what information the service collects, how it is used, with whom it is shared and for what purpose, the safeguards that are in place to protect it and how service users can access information held about them.

Appendix 1 – What a statement of information practices should contain

What is a statement of information practices?

A statement of information practices is a generic document made available to service users. It should set out, at a high level, what information the service collects, how it is used, with whom it is shared and for what purpose, the safeguards that are in place to protect it and how service users can access information held about them. It should be clearly displayed in hospitals, GP surgeries and by all other health and social care providers outlining all information practices undertaken by that particular service.

As a general rule, information should only be used for the primary purpose for which it was collected. Primary purpose relates to information which has been collected and is being kept by a custodian for the purpose of protecting, promoting, maintaining or meeting the physical and mental health needs of an individual.[1] Secondary use of information relates to information collected in the course of providing care, being used for purposes other than direct service-user care. Service user data can be used for many valuable secondary purposes, which bring benefits to the service-user population as a whole. In general, National Health Information Resources (NHIR) collect secondary data.

A service provider, such as a hospital, should have a generic statement of information practices that describes generally how information is used for both primary and secondary purposes. The following sections outline questions that should be addressed in a statement of information practices.

What personal health information is collected?

This section should outline the type of personal health information that the organisation collects and how it is collected. For example it should outline that demographic information such as name, address and date of birth is collected in addition to health information such as medical history and test results. The manner in which such information is collected and recorded should also be documented – for example it is collected directly from service users in many cases but may also be sourced from another healthcare provider, for example a GP may forward patient details to a hospital to which it has referred a patient for a particular procedure. The fact that information is recorded in the course of providing treatment or a service and how this information will be stored should also be documented. Personal information collected for secondary purposes should also be outlined.

How is personal information used?

The purposes for which such information is collected and how it is used should be clearly documented here. This section should include clear examples such as that information is used to manage the service users care (primary purposes) or that it may be used for secondary purposes, for example, for quality improvement purposes (such as clinical audit) or to plan and manage services. Instances in which personal information is shared should also be documented here – for example referral of a service user to a specialist. Any potential secondary uses of information,

the associated benefits of such uses and the right of data subjects to refuse consent to such uses should also be included.

What is the consent process?

This section should clearly define consent and the scenarios in which consent should be obtained from service users. Particular attention should be given to secondary uses of information and the right of service users to opt out of such uses. The fact that some secondary uses are permitted without consent under legislation – such as information being collected by the National Cancer Registry – should also be documented. Once information has been fully anonymised the provisions of the Data Protection Acts no longer apply, which means that it is not necessary to obtain consent to use the data. However, the Data Protection Commissioner advises that service users should still be informed, which can be achieved through the statement of information practices. The process for obtaining the data subject's consent for the use of their personal information should be outlined. This section should encourage data subjects to raise any issues or concerns they may have during the process.

How is the privacy of personal information protected?

This section should outline (at a high level) the safeguards put in place by the service provider to protect the data subjects' personal information. Safeguards include role-based access controls, anonymisation of data for secondary use, security policies and procedures, staff training in the appropriate handling of information and regular audits of compliance, and the completion of privacy impact assessments. Assurances should also be provided around the information transmission to National Health Information Resources that use the data for secondary purposes.

What are the rights of the service user/data subject?

This section should document the right of service users/data subjects, for example under Data Protection[1;2] and Freedom of Information legislation,[3;4] to access personal information held about them and have any factual inaccuracies corrected. The fact that the same right applies to data subjects in terms of information held by National Health Information Resources should be highlighted. The procedure for making such an access request should also be clearly set out in this section.

How can the service user/data subject obtain further information?

Service users/data subjects should be made aware of how they can obtain further information on the service provider's information handling practices or on any of the information set out in this document.

What is the procedure for making a complaint?

Information should be provided on how a service user/data subject can make a complaint about, for example, the manner in which their information was collected or consent was obtained, a use of their information to which they have not consented or any concerns they may have about the service provider's information handling practices.

Appendix 2 – Role of the Health Information and Quality Authority in relation to information governance

The National Health Information Strategy 2004 (NHIS) calls for the development of a framework for information governance.[38] The strategy states, within this action, that a specialist function for information governance will be established by the Health Information and Quality Authority.

The 2001 report by the Department of Health and Children – *Quality and Fairness, A Health System for You*[39] – specifies that the Department of Health and Children will publish a Health Information Bill[40] which will provide a legislative basis for information governance to support health and social care professionals in managing personal health information. The Bill will also recognise the rights of service users, health and social care professionals and service providers. The Department of Health and Children published a *Discussion Document on the Health Information Bill* in June 2008.[18] It is expected that the Bill will build on existing legislation including the Data Protection and Freedom of Information Acts. Once enacted, this legislation will form the legal basis for health information governance in Ireland.

Under section (8)(1)(k) of the Health Act 2007, the Health Information and Quality Authority (the Authority) has responsibility for setting standards for all aspects of health information, and monitoring compliance with those standards. In addition, the Authority is charged with evaluating the quality of the information available on health and social care – section (8)(1)(i) – and making recommendations in relation to improving the quality and filling in gaps where information is needed but is not currently available – section (8)(1)(j). A number of national standards set by the Authority require service providers to have effective arrangements in place for information governance.

In line with the NHIS and the provisions in the Health Act 2007, the development of guidance to support information governance has been identified as a priority for the Authority. This work has been completed in accordance with the provisions of the Health Information Bill and informed by feedback following consultation with stakeholders. The aim of this guidance is to support service providers in complying with the Authority's *National Standards for Safer Better Healthcare* and to be a resource to assist them in improving their information governance practices.

In 2011 the Authority published a guide on information governance, called *What you should know about Information Governance: A Guide for health and social care staff*.[42] The guide was a first step in raising awareness of information governance among all health and social care staff and to highlight the importance of handling personal health information legally, securely, efficiently and effectively. The guide was aimed at staff of all levels and was widely circulated with the intention that it would be available as a resource anywhere that personal health information is collected to promote a culture of good information governance practices within services.

The Authority also developed and launched an information governance self-assessment tool[43] in 2011. The tool is designed to be used by management internally to help services to meet the baseline requirements for information governance. The tool is available to download on the Authority's website www.hiqa.ie.

Appendix 3 – Methodology for guidance development

The Authority developed this guidance on information governance following a review of national and international practice in relation to information governance in health and social care services. These reviews were published and are available on our website www.hiqa.ie and include:

- An *'As Is' Analysis of Information Governance Practices in Health and Social Care Settings in Ireland*[44] which identifies and documents current practice in relation to information governance in Ireland.
- *International Review of Information Governance Structures*[45] which identifies relevant legislation and national and local structures that support information governance in selected countries.
- *International Review of Health Information Governance Management*[46] which identifies management structures that are in place to support information governance within services in selected countries.
- *International Review of Data Quality*[47] which identifies standards and other initiatives to support data quality in health and social care in selected countries.
- *Guidance on Privacy Impact Assessment in Health and Social Care*[48] which was developed as a resource to support service providers protect the privacy of their service users and to strengthen governance arrangements around health information. A privacy impact assessment (PIA) is a tool that is used to evaluate the privacy implications of projects that involve the collection, use, storage or disclosure of personal health information. Where potential privacy risks are identified steps are taken to avoid or mitigate these risks.
- *International Review of Information Security*[49] which details what security measures are in place internationally to protect personal health information.
- *International Review of Secondary Use of Personal Health Information*[50] which details how other countries safeguard personal health information when it is being used for secondary purposes not directly related to the care process.

The main findings from these reviews are:

1. It is fundamentally important to implement an appropriate governance and management structure to support information governance in an organisation. This includes the following:
    - having executive level responsibility, accountability, leadership and effective management in place to support information governance
    - having policies and procedures in place to support information governance
    - training and education of staff
    - self-assessment and continuous improvement.

2. The subject of information governance is quite broad but in order to bring coherence, transparency and assurance to information initiatives in health and social care settings, what information governance does and does not include should be clearly defined. Information governance involves implementing the necessary governance and management structures to ensure that data quality, privacy and confidentiality, information security and the secondary use of information can be assured.

Appendix 4 – List of useful resources and legislation

Please note that the accuracy, quality and relevance of these works is not guaranteed by the Authority and more recent information may have superseded these works. It is not intended to be an exhaustive list. It is the responsibility of service providers to identify the best available evidence relevant to their activities.

Resources

Department of Finance: Centre for Management and Organisation Development. *Protecting the Confidentiality of Personal Information*

FOI Central Policy Unit, The Department of Finance. *A Short Guide to the Freedom of Information Act 1997 and Freedom of Information (Amendment) Act 2003*

Irish College of General Practitioners. *A Guide to Data Protection Legislation for Irish General Practice*

Irish College of General Practitioners. *No Data, No Business: Information Communications Technology (ICT) Security Guidelines*

Medical Protection Society. *The Medical Protection Society's Guide to Medical Records in Ireland*

Council of Europe. *Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data*

Health Information and Quality Authority. *Guidance on Privacy Impact Assessment in Health and Social Care.* 2010

Health Information and Quality Authority. *What you should know about Information Governance – A Guide for health and social care staff. 2011*

National Hospitals Office. *Code of Practice for Healthcare Records Management.* 2007

Office of the Data Protection Commissioner. *Data Protection (Amendment) Act 2003 - A Summary Guide.* 2003

Office of the Data Protection Commissioner. *Data Protection Guidelines on Research in the Health Sector.* 2007

The Office of the Data Protection Commissioner. *Data Security Guidance*

ISO/IEC 17799:2005 *Information Technology – Security techniques – Code of practice for information security management.*[24]

ISO/IEC 27003:2010 *Information Technology – Security techniques – Information Security Management Systems – Requirements.*[25]

Useful websites

www.dataprotection.ie

www.oic.gov.ie

www.hiqa.ie

This list is not exhaustive and is not intended to include all the legislation that may be relevant to service providers. It is the responsibility of service providers to identify the legislation relevant to their activities.

Legislation

Bunreacht na hÉireann. 1937

Data Protection (Access Modification) (Health) Regulations, 1989

Health (Provision of Information) Act, 1997

Infectious Diseases (Amendment) Regulations 2011

Infectious Diseases (Maintenance) Regulations, 1981

Data Protection (Amendment) Act 2003

Data Protection Act, 1988

Freedom of Information (Amendment) Act 2003

Freedom of Information Act, 1997

Health Act 2007

Health Act, 1947

Statistics Act, 1993

Notes

Notes

For further information please contact:
Health Information and Quality Authority,
George's Court, George's Lane, Dublin 7
Phone: +353 (0)1 814 7400
Email: info@hiqa.ie
URL: www.hiqa.ie

Published by the Health Information and Quality Authority