Health Information and Quality Authority

An tÚdarás Um Fhaisnéis agus Cáilíocht Sláinte

Health Information and Standards

Public consultation: Draft recommendations on a consent model for the collection, use and sharing of health information in Ireland

November 2021

Safer Better Care

About the Health Information and Quality Authority (HIQA)

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

HIQA's mandate to date extends across a wide range of public, private and voluntary sector services. Reporting to the Minister for Health and engaging with the Minister for Children, Equality, Disability, Integration and Youth, HIQA has responsibility for the following:

- **Setting standards for health and social care services** — Developing person-centred standards and guidance, based on evidence and international best practice, for health and social care services in Ireland.
- **Regulating social care services** — The Chief Inspector within HIQA is responsible for registering and inspecting residential services for older people and people with a disability, and children's special care units.
- **Regulating health services —** Regulating medical exposure to ionising radiation.
- **Monitoring services** — Monitoring the safety and quality of health services and children's social services, and investigating as necessary serious concerns about the health and welfare of people who use these services.
- **Health technology assessment** — Evaluating the clinical and cost-effectiveness of health programmes, policies, medicines, medical equipment, diagnostic and surgical techniques, health promotion and protection activities, and providing advice to enable the best use of resources and the best outcomes for people who use our health service.
- **Health information** — Advising on the efficient and secure collection and sharing of health information, setting standards, evaluating information resources and publishing information on the delivery and performance of Ireland's health and social care services.
- **National Care Experience Programme** — Carrying out national service-user experience surveys across a range of health services, in conjunction with the Department of Health and the Health Service Executive (HSE).

Overview of the health information function of HIQA

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

Safe, reliable healthcare depends on access to, and the use of, information that is accurate, valid, reliable, timely, relevant, legible and complete. For example, when giving a patient a drug, a nurse needs to be sure that they are administering the appropriate dose of the correct drug to the right patient and that the patient is not allergic to it. Similarly, lack of up-to-date information can lead to the unnecessary duplication of tests — if critical diagnostic results are missing or overlooked, tests have to be repeated unnecessarily and, at best, appropriate treatment is delayed or at worst not given.

In addition, health information has an important role to play in healthcare planning decisions — where to locate a new service, whether or not to introduce a new national screening programme and decisions on best value for money in health and social care provision.

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

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

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

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

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

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

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

Table of contents

Background to recommendations

A major challenge for healthcare in Ireland today is striving to achieve an appropriate balance between the protection of personal health information and the use and sharing of such information to improve care. Advances in digital technologies have the potential to improve the quality of care provided to patients and also promote better use of resources. This also means that, as plans advance towards a more digital healthcare system, vast amounts of health information will be available to use and share electronically. A recent national public engagement in Ireland on this topic identified that individuals welcome a move towards the use of electronic records; however, they want to be more informed about when, and how, their information is shared and how privacy is protected.[2]

Currently, in Ireland, there is no overarching legislative framework to support the safe and effective use of personal information in health and social care. The collection, use and sharing of personal information is essential for high-quality and safe care as health professionals need relevant patient information available to them when making clinical decisions. Individuals also expect healthcare professionals and organisations to communicate effectively with each other and use their information to manage and govern the health system. However, there needs to be clarity around when and how personal information can be collected, used and shared by health and social care services. There is also a need to promote adequate security measures to protect against known and potential risks associated with collecting, using and sharing both paper-based and electronic health records (EHRs).

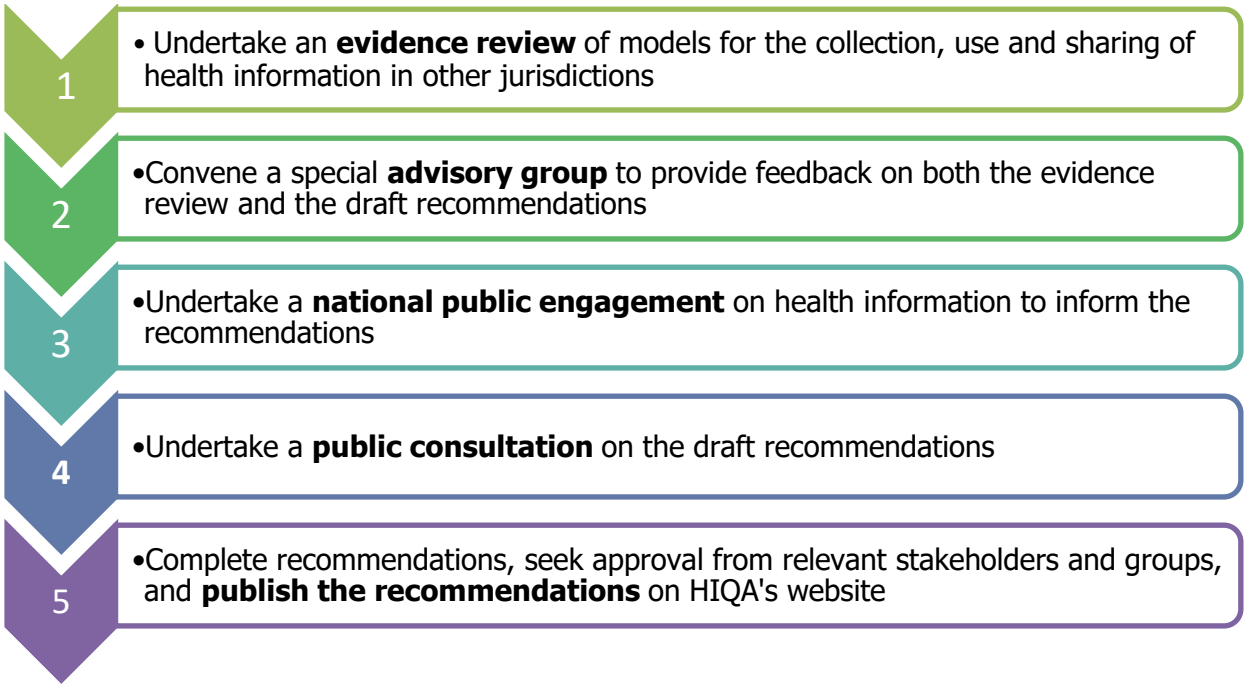
HIQA is developing recommendations on a consent model for the collection, use and sharing of health information in Ireland. Consent for the use of personal information is a process by which a person expresses that they are willing for their information to be collected, used and shared.[3] These draft recommendations have been published for public consultation to ensure that members of the public have an opportunity to engage in, feedback on, and inform the final recommendations.

The draft recommendations were developed as per HIQA's legislative remit under the Health Act 2007 and subsequent amendments to the Act.[1] Under the Health Act 2007, HIQA has a statutory remit to develop standards, evaluate information and make recommendations about deficiencies in health information. The responsibilities of HIQA in this regard are outlined in the following sections of the Act:

- Section 8(1)(i): to evaluate available information respecting the service and the health and welfare of the population.
- Section 8(1)(j): to provide advice and make recommendations to the Minister for Health and the HSE about deficiencies identified by HIQA in respect of the information referred to in paragraph (i).

Stages to development of recommendations

The recommendations were developed in line with the methodology outlined in HIQA's Health Information and Standards Quality Assurance Framework and include the following stages:



Stage 1: Evidence review - At the initial stage of the development process, HIQA undertook a review of consent models for the collection, use and sharing of health information to identify examples of best practice internationally (click here for review). Experts in each of the eight jurisdictions were contacted for interview to ensure the most relevant and up-to-date information was gathered. An update, as well as a more detailed review, was completed in 2021 by undertaking another desktop review and contacting experts in each country to validate the information. The eight jurisdictions included in the reviews were:

- Australia
- Denmark
- England
- Estonia
- Finland
- New Zealand
- Northern Ireland
- Ontario (Canada).

In addition, an evidence synthesis paper was developed to support these recommendations which includes an 'as-is' analysis of the current health information landscape in Ireland and a summary of the latest international evidence.[4] The

significance of the key findings from the evidence synthesis will be discussed in this document.

Stage 2: Advisory group - An advisory group was convened four times to provide assistance in developing the recommendations (see **Appendix 1** for list of members). Advice and guidance was sought from the advisory group at each stage of the recommendations development process.

Stage 3: National public engagement - HIQA, in partnership with the Department of Health and the Health Service Executive (HSE), undertook a national public engagement to guide the development of the recommendations in 2020-2021. The aim of the national public engagement on health information was to understand the opinions and attitudes of the Irish public in relation to the collection, use and sharing of personal health information. A survey was conducted with 1,200 members of the public to give their feedback on how their personal health information is collected, used and shared by health and social care services, and their opinions on the use of digital technologies in this area. In order to further understand the findings of the survey, 14 focus groups were held with the public, patients and representatives of different service user groups. The full report, *Findings from the National Public Engagement on Health Information*, can be found on HIQA's website, here. The findings of the national public engagement on health information were used to inform these recommendations.

Stage 4: Public consultation - Based on the findings from the evidence review and engagement with stakeholders, the project team prepared a draft set of recommendations for public consultation. The advisory group reviewed the draft recommendations prior to the public consultation.

Stage 5: Next steps (approve and publish recommendations) – After the public consultation, the recommendations will be reviewed and amended to reflect the feedback. The updated draft recommendations will then be circulated to the advisory group for final considerations. Following analysis and review of the additional feedback, the final recommendations document will be completed and sent for approval to the HIQA Executive Management Team, before final approval by the HIQA Standards Information Research and Technology (SIRT) committee, a sub-committee of its Board, and then the HIQA Board. After the HIQA Board has approved the recommendations, they will be submitted to the Minister for Health and will also be published on the HIQA website.

Scope of recommendations

The recommendations on a consent model for the collection, use and sharing of health information in Ireland include the following:

1. Key definitions to support a consent model, including a definition for health information, the use of information for direct care, and the use of information beyond direct care
2. The circumstances when consent is required from individuals for the collection, use and sharing of their personal information (the consent model)
3. The legislative requirements for health information
4. The governance structures necessary to ensure that personal information is processed appropriately and securely in line with individuals' preferences
5. The technical and operational considerations to support the consent model
6. The requirements for effective public engagement to inform decisions on how information is collected, used and shared

In scope: The scope of the recommendations is to address the consent model that should be in place for the collection, use and sharing of health information, which has been processed for the purposes of providing direct care and subsequently used for reasons beyond direct care, such as for public health and health services management and planning.

Out of scope: Legislation has been enacted in Ireland in respect of the processing of personal information for research purposes (Health Research Regulations 2018),[5] through formal applications for a consent declaration to the Health Research Declaration Committee (HRCDC). Therefore, the processing of personal information for research purposes without consent is not included in the scope of these recommendations. However, to fully describe the consent model for health information, the use of information for research purposes is discussed throughout the evidence synthesis.

For the remainder of this document:
Personal information will be used to describe any data or information relating to an identified or identifiable individual. An identifiable individual is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.

Health information will be used to describe health and social care information, and as defined in Recommendation 1.

Consent for the use of health information will be used to describe the process by which a person is willing for their information to be collected, used and shared.

Introduction

The collection, use and sharing personal information in a secure manner is an integral part of health and social care provision; it is critical both for managing direct care and also for reasons beyond direct care, such as for health service planning and management, policy-making and research. Improved sharing of health information can ensure a more efficient health service by providing information when, and where, needed.[6] eHealth initiatives, such as EHRs, aim to achieve this; however, in doing so, it is also important to ensure that individuals are fully informed about the potential uses of their data and that they have a good understanding of how, and why, it may be used. Every individual should feel confident that their personal data and information will be used and protected appropriately.

For high-quality and safe care, it is in an individual's best interests that their health information is collected, used and shared appropriately. When professionals do not have access to the most relevant and up-to-date health information, it results in duplication of efforts and suboptimal delivery of care, as well as being inconvenient as individuals have to continuously repeat their medical history during consultations. More crucially, however, the lack of access to timely data and information can often lead to tests and scans needing to be repeated, which can delay care and treatment, as well as increasing costs and impacting on efficiency of services.[6] Using health information for reasons beyond direct care in a safe and controlled manner also has many significant public and societal benefits. For example, information is used by management within health services to review waiting lists and organise resources, such as hospital operating theatres, to ensure they are used to full capacity. Furthermore, information can be used to review care processes across large numbers of patients to understand the circumstances which lead to the best care outcomes. This learning can be used to develop guidelines to promote optimal care for all patients, such as in the development and implementation of national clinical guidelines.[7]

These benefits are only appreciated when health information is processed safely in a way that protects the privacy of individuals. In some situations, it is important to ask individuals if they are happy for their personal information to be used and shared. In the General Data Protection Regulation (GDPR),[3] this is referred to as seeking consent for processing of personal data.* It is important to note that under GDPR, if health information is changed to make it difficult or impossible to identify the individual about whom the data was collected, consent may not be required. For example, personal or identifiable information can be removed before sharing this information and other de-identifying techniques can be used to prevent re-identification.[8] This means that, with

* Under the GDPR, health data is considered a special category of personal data and there are specific conditions attached to its processing. Article 9 of the GDPR specifically deals with the processing of special categories of personal data, including data concerning health which can be used and shared for a number of specific reasons. For example, if processing is necessary for reasons of substantial public interest.

the correct data governance, the data can then be used in a safe and secure manner, ensuring privacy is protected.[9] A consent model should clearly outline the circumstances when consent is, and is not, required from individuals for the collection, use and sharing of their information. The processing of health information should follow a rights-based approach, meaning that an emphasis is placed on protecting and promoting people's rights and respecting their autonomy, privacy, dignity, and their values, preferences and diversity.[10]

Consent for processing of data, as defined in GDPR, is: 'any freely given specific informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'.[3]

Traditionally, models of consent are referred to as:

- Explicit consent or opt-in — an individual actively agrees or signs up to allow for data to be collected or used;
- Implied consent or opt-out — agreement can be reasonably inferred and data will be collected and used automatically unless an individual actively asks for the information not to be used or shared for a particular reason.

Involving people in important decisions about their health information and ensuring that their rights in relation to personal information are upheld is crucial, and will ensure that new technologies and initiatives, such as EHRs and citizen health portals, are implemented in a way that is acceptable. There needs to be open communication and ongoing engagement with the public around how, and why, personal health information is collected, used and shared. Public engagement must be undertaken in a meaningful and authentic way to build trust, confidence and awareness surrounding the benefits of using and sharing health information. Ongoing deep and meaningful engagement will help to design a model for health information in Ireland which will evolve to meet individuals' needs and requirements.

The following chapters outline what is needed to develop and implement a consent model for the collection, use and sharing of health information:

- **Chapter 1:** Definitions of key terms for health information
- **Chapter 2:** Consent model for health information
- **Chapter 3:** Legislation for health information
- **Chapter 4:** Governance structures to support the consent model and health information legislation
- **Chapter 5:** Technical infrastructure and operational considerations
- **Chapter 6:** Public engagement on health information

The recommendations have been informed by international evidence, a review of the current situation in Ireland, and engagement with a broad range of national and

international stakeholders. See the associated evidence synthesis paper for an 'as-is' analysis of the current health information landscape in Ireland and a detailed description of the international evidence that has informed these recommendations.[4]

Chapter 1 – Definitions to support a consent model

This section describes the approaches that eight other jurisdictions, as outlined in the accompanying evidence synthesis,[4] have taken when defining key terms for health information and the concepts that are considered important when defining each term. This has informed the development of the recommended definitions for these terms for an Irish context.

Health information

All jurisdictions reviewed define health information, to some extent, in national legislation although the level of detail varies. For example, Estonia has a simple definition where health information relates to "personal data required for the provision of a health service, data related to the state of health of a data subject, and data related to health care".[11,12] In contrast, New Zealand provides a detailed list of the type of information that is classed as health information, including medical history, donation of bodily parts, and information on disabilities.[13] Some jurisdictions have specifically included a reference to how information is recorded.[14-18] The key concepts included in current definitions across jurisdictions reviewed were: a) individual health status and condition, incorporating both physical and mental health; b) health and social care provided to an individual; and c) other personal information collected to provide health and social care, such as name and date of birth.

Use of health information for direct care

The use of health information to inform the provision of direct care is cited as its primary purpose in all of the jurisdictions examined in this review. There are differences, however, across jurisdictions on what activities are considered direct care. In some jurisdictions, activities that inform the wider provision of care are considered sufficiently connected to the provision of direct care once they are conducted by someone with a 'legitimate care relationship' to the individual. A legitimate care relationship is one where a health or social care professional is involved in informing the direct care of an individual. For example, in Northern Ireland, clinical audits and case reviews carried out by members of the care team are considered to have sufficient connection with direct care to be viewed as a primary use of health information.[19] The use of health information in emergency situations where it is necessary to lessen or prevent a serious threat to an individual's life, health or safety is also viewed as a critical element of direct care.

Use of health information for beyond direct care

The majority of jurisdictions included in the review do not specifically define the use of health information beyond direct care in their legislation; only Finland and Northern Ireland were found to define this use of health information in legislation and both refer to it as 'the secondary use' of health information.[14,19] All jurisdictions outline the

permitted uses of health information beyond direct care in legislation, although the depth of detail differs between jurisdictions. The permitted uses of health information beyond direct care vary across jurisdictions. Health service management and monitoring, planning and administration, quality improvement activities, health research, public health, health and social care statistics, and training and education are the most common uses of health information beyond direct care. A number of additional uses were also identified that are unique to particular jurisdictions.

Currently, in Ireland, these terms are not defined in legislation. It is important that there is a consistent understanding of these terms in the development of a consent model for health information. HIQA performed a review of the legislation in the eight jurisdictions included in the international review in order to draft definitions for each of these terms. These were subsequently refined for the Irish context after feedback from the advisory group.

1.1 Recommendations – key definitions to support a consent model

HIQA makes the following recommendations:

Definitions	
1.	Based on a review of international best practice and stakeholder consultation, HIQA recommends that the following terms are defined in legislation: **Health information** is "information[†] which relates to the physical or mental health or condition of an individual; the health or social care that is being, has been, or may be provided to an individual, or an individual's expressed wishes about the future provision of health or social care; and other personal information required for the provision of health or social care". The use of **health information for direct care** is "information used to inform the provision of direct care to an individual; activities that focus on improving direct care and are undertaken by health and social care professionals with a legitimate care relationship,[‡] such as case reviews and local clinical audit; and emergency situations where information use is necessary to lessen or prevent a threat to an individual's life, health or safety". The use of **health information beyond direct care**[§] is "information used and shared by health services and health service providers for activities that contribute to the overall provision of health and social care to a population as a whole, or a group of individuals with a particular condition, but which fall

[†] Information sources includes a wide variety of material, including but not limited to: handwritten notes; electronic records; correspondence, including oral correspondence, between health and social care professionals; visual and audio recordings; laboratory report; and communication with patients and services users (including oral communication, texts and emails).
[‡] A legitimate care relationship is one where a health and social care professional is involved in informing and delivering the direct care of an individual.
[§] Explicit consent is required for the use of personal information for reasons beyond direct care (except where exemptions apply). Anonymised or aggregated data should be used when the purpose of use can be achieved without personal information, even when exemptions apply.

	outside the scope of direct care. Uses beyond direct care include: health services management and planning, health and social care research, public health, statistics, and training and education.”

Chapter 2 – Consent model for health information

Rights-based approach for health information

The processing of health information should follow a rights-based approach, meaning that an emphasis is placed on protecting and promoting people's rights. This involves respecting their privacy but also their autonomy, dignity, values, preferences and diversity.[10] Data protection is a fundamental right set out in Article 8 of the European Union (EU) Charter of Fundamental Rights.[20] Under the GDPR, health data is recognised as a special category of data, due to its sensitive nature, giving it more stringent protections than other types of personal data. Therefore, the GDPR details specific rights of individuals in respect of their personal data. These include, but are not limited to:

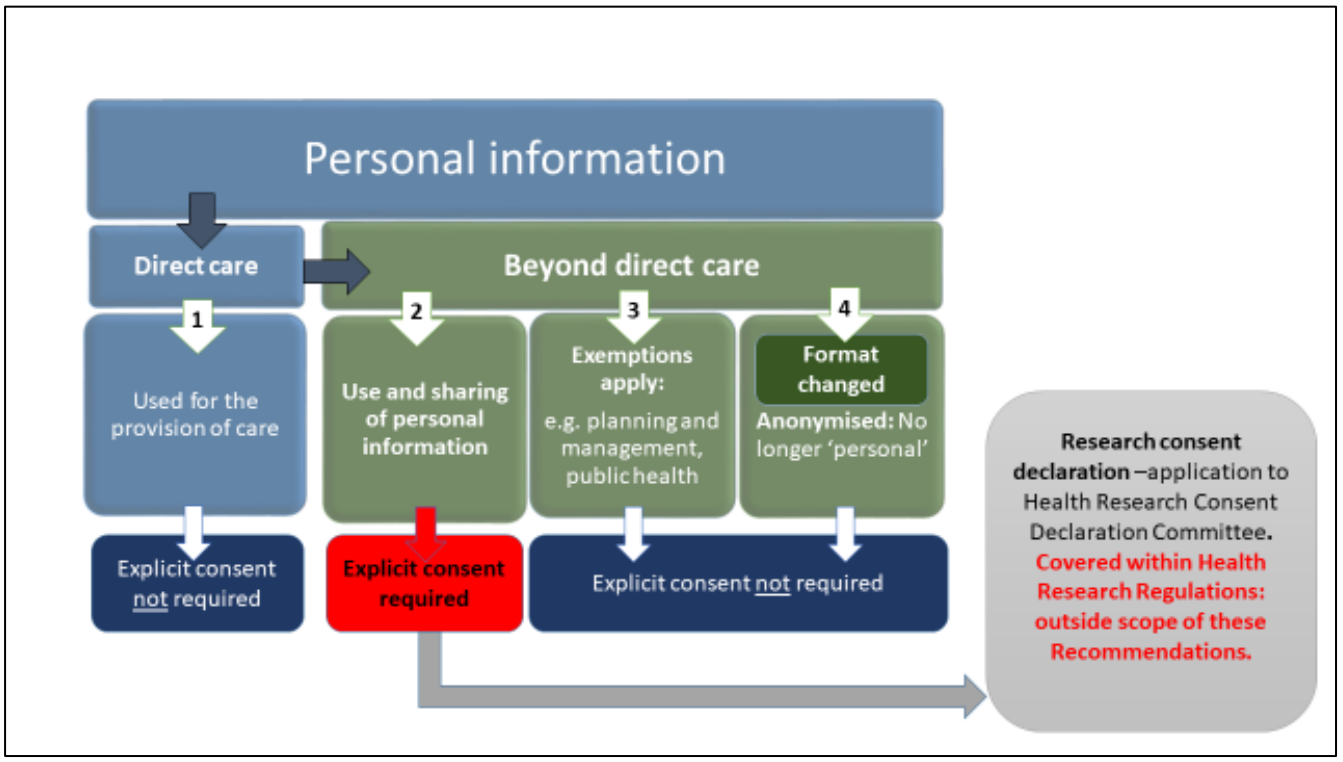
- Right to access - request a copy of any of their personal data which are being used in any way
- Right to be informed (transparency) - clearly outlining the specific purposes for which personal data are used in any way
- Right to rectification - to have inaccurate personal data rectified, by the controller, without undue delay
- Right to object - to certain types of processing of personal data.

It must be noted that data protection is not an absolute right.[21] It must always be balanced against other values, fundamental rights, human rights, or public and private interests. As this is the case, it can be confusing for individuals to understand the circumstances under which there may be grounds for them to exercise their data protection rights. Therefore, as technologies develop and the potential to use and share health information increases, the rights of individuals in relation to their personal information should be openly discussed, as well as the choices they have about this.

Consent model for health information

A consent model for health information should clearly outline the situations in which individuals' consent is, and is not, required for the use of personal information in health and social care. The international review presented in the evidence synthesis identified that although there are similarities across the jurisdictions reviewed, each jurisdiction has contextual differences which prevent the same approach being adopted consistently, although the basic principles are common.[6] The proposed consent model, informed by the evidence synthesis, is outlined in **Figure 1**.[6]

Figure 1: Consent model for personal information



Category 1: Use of information for direct care

In all jurisdictions reviewed, and in Irish and European legislation, the processing of personal information is lawful for the provision of care. This means that health and social care professionals can use and share health information to provide safe and effective care to individuals. Some jurisdictions have also incorporated explicit rules regarding the transparency of the use and sharing of personal information. For example, in Northern Ireland, a *Code of Practice on Protecting the Confidentiality of Service User Information* has been developed which states that service users must be informed of the information sharing necessary to provide direct care.[19]

Category 2: Use of information beyond direct care (explicit consent)

If personal information is required for reasons beyond direct care, explicit consent for the use and sharing of personal information is required. This approach is common across all jurisdictions and is based on the principle that personal information should only be used for the purpose for which it was collected.

Category 3: Use of information beyond direct care (consent exemptions apply)

All jurisdictions reviewed include provisions in their data protection acts to allow, in certain circumstances, personal information to be used for reasons beyond direct care without explicit consent. For example, for planning and management of services, and public health. The use of personal information for these specific and defined reasons without the requirement for consent are referred to as '*consent exemptions*'. There is no

standard approach to defining exemptions across jurisdictions, although the following activities are generally included: situations where the information is required for statute, court or tribunal proceedings; or where there is an overriding public interest or value in the use or sharing of the information. Therefore, consent exemptions need to be clearly outlined in legislation, and in associated regulations and guidance. See **Appendix 2** for examples of exemptions and potential data sharing and linkage activities that may be possible if the proposed consent model is implemented, including the appropriate legislation, governance structures, technical infrastructure and operational capacity.

Category 4: Use of information beyond direct care (anonymised)

The use and sharing of health information for purposes beyond direct care, such as for health and social care planning, and policy development, does not always require personal information. All jurisdictions reviewed have provisions in place to allow anonymised health information to be used for reasons beyond direct care without the requirement for explicit consent. This is because irreversibly and effectively anonymised information is no longer considered personal information.[8]

In jurisdictions with well-developed structures for the use of information for purposes beyond direct care, specific agencies are assigned responsibility for governing and managing the anonymisation process and the use and sharing of this information. These agencies have a role in managing data requests and have expertise in the latest anonymisation and linkage techniques. When such data governance structures and technical infrastructure are in place, existing data and information can be linked, anonymised and shared securely ensuring the optimal use of data to inform policy and practice, and to support innovation (this will be discussed further in Chapters 4 and 5).

Research consent declaration: It is recognised in Ireland, similar to other jurisdictions, that in limited situations, obtaining consent will not be possible and that the public interest of doing some research projects significantly outweighs the need for explicit consent. In Ireland, in this instance, it is possible to apply for a consent declaration where the HRCDC reviews applications and can permit the use of personal data without consent for research purposes in exceptional circumstances. The HRCDC was established as part of the Health Research Regulations developed under the Data Protection Act, 2018.[5] The purpose of the regulations is to support health research and promote necessary and desirable public confidence in such research, providing for an independent and representative committee to make decisions on such applications.
Note: The use of personal information, with a consent declaration, for research has been included in this consent model for the purposes of presenting a complete understanding of the different uses of health information. However, as Health Research Regulations 2018 have been enacted in Ireland, the use of personal information in this instance, for research purposes without seeking explicit consent, is not included in the scope of these recommendations.

Consent preferences

The process of seeking consent for health information is evolving in many jurisdictions, particularly where eHealth systems are more advanced. Consent can involve a once-off or a fixed arrangement, or it can be a dynamic process which allows the individual to have more control over their preferences. Dynamic consent is a model that involves ongoing engagement, and enables people, usually through an interactive digital interface, to express their consent preferences and how these might change over time. This approach has been explored primarily within medical research, in fields such as bio-banking and genomics, where ongoing contact is required with participants.[22] It is now also being used in the area of health information as individuals are increasingly provided with opportunities to actively manage consent preferences regarding the use and sharing of their personal health information through online portals; this involves ongoing engagement and communication between individuals, and the users and custodians of their information.[23]

Although consent is not required by law for the use of personal information for the provision of care, some jurisdictions reviewed provide individuals with a level of control over how their personal information is used for direct care. For example, in Ontario (Canada),[24] Estonia,[25] and Australia,[26] individuals can request that aspects of their medical records are not viewed, used and shared by healthcare professionals without their consent. In such instances, individuals are informed that blocking access to certain information may impact on their direct care as the care professional may not be able to make a fully informed decision. In Ontario (Canada), individuals can request that a 'consent directive' is added to the record, meaning that certain information will be blocked on the record and can only be accessed once consent has been granted by the individual, or in an emergency situation (this will be discussed further in Chapter 5).

To date, in most jurisdictions reviewed, an opt-out consent approach has been used for the setting up of EHRs. For example, in Australia, there was a six-month period (July 2018 – January 2019) during which all individuals had the opportunity to decide if they wanted a My Health Record and to opt-out if they did not want one.[23] Electronic records were subsequently created for all eligible Australians who did not opt-out. If individuals later decide that they do not want a My Health Record, they can cancel it at any time, and their record will be permanently deleted. Individuals that have opted-out of having a My Health Record can change their mind and decide to register at any time.

Internationally, there is currently ongoing debate about the advantages and disadvantages of this approach.[27-29] Among proponents of an opt-in consent approach to initiation of national EHRs, most arguments against the opt-out approach for EHRs centre on the security of health data in centralised record systems.[27,28] In some jurisdictions, there has been a move away from opt-in approaches due to poor uptake.[30] Without high levels of uptake, there is a risk that the advantages an EHR can offer will not be realised, such as higher quality and safer care due to improved access to

accurate, up-to-date, and complete information at the time of care, and improved communication between healthcare providers as well as individuals.[31] In addition, both opt-in and opt-out consent approaches for EHRs may be associated with a patient safety risk as if a person refuses to opt-in, or chooses to opt-out, of having one, their clinical information will not be available to clinicians when they need it. This has the potential to result in sub-optimal decision-making, particularly during emergencies.[29] As such, it is important that countries take into account multiple factors and perspectives when deciding on what consent approach to take when implementing EHRs, or other significant eHealth initiatives. In Ireland, effective public engagement will be required to identify the approach that meets the needs of citizens and to maintain public trust throughout the process (public engagement will be discussed further in Chapter 6).

In some jurisdictions, individuals can also review and express their consent preferences for how their information is used beyond direct care, usually through a portal or other online process. The approaches taken, and the activities which an individual can opt-out of having their information used vary between jurisdictions. In England, for example, under the 'national data opt-out', individuals can opt-out of their personal information, collected by the NHS, being used for research and planning, but an individual does not have the option to opt-out of their de-identified information being used for these purposes.[32] In Australia, however, individuals can opt-out of their de-identified health information being shared for public health and research purposes.[33]

In order to provide individuals with greater control over their health information, the appropriate technical infrastructure is needed to enable a dynamic method to offering choices and to allow individuals manage their consent preferences. In most cases, the infrastructure to control the use and sharing of one's personal information is delivered through a portal, with the exception of England which, in the absence of a citizen health portal, has developed a specific online platform (the technical infrastructure to manage consent preferences will be discussed further in Chapter 5).

2.1 Recommendations – consent model for health information

HIQA makes the following recommendations:

Rights-based approach to implementing a consent model	
2.	The collection, use, and sharing of personal information should follow a **rights-based approach.** In all circumstances, individuals should be informed of: ▪ how, and why, their personal information is being, or may be, collected, used and shared. ▪ their rights to privacy and confidentiality in relation to their personal information, and what choices they have about this. To support a rights-based approach, it is important that everybody working in the health and social care system understands their responsibilities and obligations in relation to the collection, use and sharing of personal

	information. In addition, a system-wide approach is needed to actively inform individuals about how their personal information is used and what individuals' rights are in relation to privacy and maintaining confidentiality (see recommendation 10).
Consent Model	
3.	Based on a review of international evidence, HIQA recommends the introduction of the following consent model for the collection, use and sharing of personal information, and that this model should be defined in legislation (see recommendation 4): **Note**: As a general principle, anonymised or aggregate data should be used in all circumstances where the purpose of use can be achieved without personal information. **Use of information for direct care** ▪ **Category 1:** Explicit consent is not required for direct care. The collection, use and sharing of personal information is lawful under the Data Protection Act 2018 [34] and the General Data Protection Regulation [3] where it is necessary for the provision of health and social care. This means that professionals with a care relationship can collect, use and share personal information to ensure they have accurate and timely information to deliver safe and effective care. However, the principles of data protection and transparency still apply, so individuals should always be fully informed of how, and why, their personal information is being, or may be, used. **Use of information beyond direct care** ▪ **Category 2:** Explicit consent is required for the collection, use and sharing of personal information for reasons beyond direct care (except where exemptions apply – see Category 3).** ▪ **Category 3:** Explicit consent is not required for the collection, use and sharing of personal information if the use is considered one of the following exemptions, as defined below: ➢ **Identification, prevention, control, and surveillance of population health and disease**: the use of information to support the identification, prevention, control and surveillance of population health and disease, including both communicable and non-communicable diseases. ➢ **Compilation or analysis of statistics relevant to health and social care**: the collection, compilation, analysis or interpretation of data, expressed in either numerical or non-numerical form, relevant to health and social care.

** In limited situations, when the public interest of doing research significantly outweighs the need for explicit consent, the Health Research Consent Declaration Committee (HRCDC) will review applications and make a final decision on the need for consent. Research Consent Declarations are covered within the Health Research Regulations and therefore are **outside of the scope of these recommendations**.

	➢ **Management and planning of health and social care services:** the use of information to inform the planning, monitoring, delivery, improvement, auditing and evaluation of health services. ➢ **Health and social care professional education and training:** the use of information to develop resource materials or the sharing of information during structured professional development activities in order to support the education and training of health and social care professionals. ➢ **Alternative legislative basis for the collection, use and sharing of personal information:** the collection, use and sharing of personal information is required by law. ○ Each exemption should be clearly defined in legislation and the permitted uses of data within each exemption should be described in supporting regulations and guidance. ▪ **Category 4:** Explicit consent is not required for the sharing of health information if the information is considered anonymised in accordance with the Data Protection Commission's 'Guidance on Anonymisation and Pseudonymisation'.(8) As advances are made in this area, there is a need to ensure that this processing occurs in a regulated and controlled environment with the appropriate governance and infrastructure in place (see recommendations 6 and 7). To support best practice, it is recommended that a code of practice is developed (see recommendation 8).

Chapter 3 – Legislation

In reviewing the legislation for health information enacted in the eight jurisdictions, HIQA found that each jurisdiction has taken a different approach to developing legislation in this area.[4] Some have included detailed provisions for health information in the data protection legislation or Health Acts, and others have developed specific legislation and associated guidance to define the rules for the collection, use and sharing of health information. Although the approaches to developing legislation for health information adopted by other jurisdictions differ, the decision to develop health information-specific legislation and codes of practice to regulate the collection, use and sharing of health information — for example by Australia, Finland, New Zealand, Northern Ireland and Ontario (Canada) — identifies a need to clearly define rules for the processing of health information, both for direct care and beyond direct care. Within the EU, GDPR provides for a harmonised approach to the processing of special categories of personal data concerning health. However, to address differences in context across jurisdictions, it is recommended that Member States develop national law to provide for specific and suitable measures to protect the fundamental rights and the personal information of citizens for health and social care.[3]

The international review found that all jurisdictions have specific details regarding the use and sharing of personal health information for direct care, either within data protection legislation or health acts, or both.[4] The data protection legislation is used as the basis for data processing in all jurisdictions, including Ireland; however, the provisions and details specifically for health information vary. The Health Acts in each country also tend to include details regarding the collection, use and sharing of health information for direct care. In England, the Health and Social Care Act 2012 places a duty to share information between professionals for the provision of health services or adult social care.[35] Similarly, Estonia's Health Services Organisation Act 2001 outlines that health information may be shared for the provision of care without explicit consent once the principles of confidentiality are maintained.[11]

All of the jurisdictions reviewed have made provisions within legislation for the use of health information beyond direct care; however, each one has approached the regulation of health information for uses beyond direct care in different ways. The data protection legislation in each country has provisions for the processing of identifiable personal information for public health purposes, and some also include provisions for the use of such information for health research purposes. Additional detail about the processing of health information for other purposes is included in relevant Health Acts or specific health information legislation. Notably, the approach taken by Finland and Australia to develop legislation and mandated frameworks for the use of information beyond direct care, or 'secondary use'[††], highlights the importance of defining structures to use and

[††] In some jurisdictions, the use of information beyond direct care is referred to as the secondary use of information.

share large volumes of information effectively and securely in a regulated and controlled environment.

In jurisdictions with advanced eHealth systems, there is either specific legislation or provisions made within existing legislation to define the collection, use and sharing of information for digital health records. For example, the My Health Records Act in Australia,[36] or the Health Act in Denmark which has a specific section for electronic records.[37] As health information becomes increasingly digitalised or electronic, these laws are vital to ensure information is collected, used and shared appropriately in line with patients' expectations and needs.

Accurate, relevant and timely health information is essential in order to improve the provision of care, to inform better decision-making, monitor diseases, plan services, inform policy-making, conduct high-quality research, and plan for future health and social care needs. In fact, many advances in healthcare depend upon the increasing availability and application of high-quality health information. In order to provide safe and effective care to the individual, health professionals need relevant information available to them when making clinical decisions.[6] Individuals also expect healthcare professionals and organisations to communicate effectively with each other and use their data to manage and govern the health system, which, in turn, promotes the safe and effective provision of patient care. However, in Ireland, the current legislative landscape for the collection, use and sharing of information is not fit for purpose.

Plans for a Health Information and Patient Safety Bill have been in existence in Ireland since 2007, but this subsequently evolved to become the Patient Safety (Notifiable Safety Incidents) Bill 2019 which primarily makes provisions for the patient safety elements contained within the original Bill. The current legislative landscape for health information in Ireland draws on a number of discrete pieces of legislation which firstly, makes it difficult to understand and navigate in a health context, and secondly, does not comprehensively cover all requirements. In particular, there are limited provisions within Irish legislation for the use of health information in relation to electronic records, or other eHealth initiatives like ePrescribing. For example, as current legislation does not have provisions for electronic prescribing, temporary amendments were enforced during the COVID-19 pandemic to ensure that patients can continue to access their ongoing treatment and 'regular' medicines. However, this temporary solution to ePrescribing is not based on international and national standards for health information.[6] In addition, the current legislation does not sufficiently address the need to use and share information across the public and private healthcare sectors. This has significant impact on direct care as healthcare professionals do not have access to timely and up-to-date patient information. It also has consequences for the planning and management of health services, and policy-making where national level data is required. Again, this was emphasised during the COVID-19 outbreak as significant resources were required to generate sufficient data to manage the response to the pandemic, particularly for contact

tracing and the vaccination programme.[6] As eHealth plans advance, there is also a need to include provisions within legislation to appropriately govern the use of information beyond direct care (this will be discussed further in Chapter 4 and 5).

In a recent position paper, published by HIQA, on the need to reform Ireland's national health information system, health information legislation was cited as one of three core enablers to achieve a robust national health information system.[6] The need for specific health information legislation is essential to advance eHealth and to implement a robust national health information system. The position paper clearly identified that the lack of legislation is hindering overall coordination between the key health information entities and organisations involved in using health information, and in particular, the collection, use and sharing of information across the public and private sector. This is vital to promote high-quality and safe health and social care services, but also to realise the huge potential and benefit to using health information beyond direct care. The ultimate goal is to collect health information once and reuse it many times for different purposes. Legislation is essential to enable the use of health information beyond direct care across all sectors including primary care, community services, and public and private hospitals. This national-level data is critical for effective planning and management of services, and policy-making. However, new legislation is the foundation that is needed to enable and ensure that information is used appropriately, and shared safely across the health and social care system (this will be discussed further in Chapters 4 and 5).

The reality is that if eHealth plans are progressed, and health and social care becomes more integrated, it will increase the potential for the collection, use and sharing of vast amounts of information. Therefore, these laws are needed urgently to ensure information is collected, used and shared appropriately. New health information-specific legislation and associated guidance on the collection, use and sharing of health information should build on existing legislation to provide clarity on implementing the consent model in practice and to outline appropriate governance structures to promote and encourage the optimal and safe use of information for wider public benefit. As this is a complex and evolving area, a legislative framework should be developed to guide recommended practice in this area to include regulations, guidelines and codes of practice. These elements are used in other jurisdictions to provide clarity on obligations and responsibilities for those working in health and social care services and to build confidence that they are processing information appropriately, as well as to develop a common understanding around individuals' rights in relation to health information (this will be discussed further in Chapter 4 and 5).

3.1 Recommendations – health information legislation

HIQA makes the following recommendations:

Legislation	
4.	Building on the data protection principles outlined in GDPR[‡‡] and in line with HIQA's recommendation in the position paper for a legislative framework in the area of health information,(6) the Department of Health should develop specific legislation in relation to the collection, use and sharing of personal information. The legislation should: ▪ incorporate the recommended definitions and proposed consent model, and promote a rights-based approach to the use and sharing of personal information (see recommendations 1-3); ▪ outline how the consent model should be monitored and regulated, addressing current arrangements and future requirements.
5.	To complement new health information legislation, a legislative framework should be developed with supporting regulations, codes of practice and policies. These supporting documents should help to define what good practice is for those working in health and social care services and to develop a common understanding around individuals' rights in relation to health information (see recommendation 8).

[‡‡] The seven data protection principles include: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability.

Chapter 4 - Governance structures for health information

The key to having a well-established health information system is having clear strategic direction. This can be achieved through the implementation of a national strategy for health information, in particular including details and associated funding for the collection, use and sharing of health information. Jurisdictions with robust governance structures at a national level tend to have advanced eHealth programmes. For example, in Denmark and Ontario (Canada), eHealth programmes are well structured with appropriate boards, groups and committees established.[38,39] They have clear roles and responsibilities and have a wide-ranging remit, with good reporting structures in place. A well-established health information system also promotes coordination and order to the management of health information. In Canada, New Zealand, England, Australia and Finland, the responsibility for a majority of national health and social care data collections is assigned to one or more specific agencies or organisations demonstrating the significance of good governance, leadership and management in the area of health information. However, in Ireland, there is currently no central body to process and make data available in an efficient manner.[40] In recent international studies in this area, in comparison to other EU and Organisation for Economic Co-operation and Development (OECD) countries, Ireland was highlighted as having poor health information infrastructure and governance, fragmented practices, and limited capabilities for using health information beyond direct care.[40,41]

HIQA's position paper on the need reform Ireland's national health information system[6] highlighted that over the past 20 years in Ireland, several strategies were published in this area, including the first national health information strategy in 2004[42] and Ireland's first eHealth strategy in 2013.[43] Many objectives that were set out in these strategies have still not been achieved. Currently, the Department of Health is drafting a new health information system strategy which is concerned with the use of data beyond direct care. In parallel, the Sláintecare§§ Implementation Strategy 2018 places a significant emphasis on the need for eHealth to enable integrated care.[44] The position paper recommended developing a health information strategy that takes a holistic and cohesive approach to managing health information, that is, how health information is collected, used and shared for direct care and also for the use of information beyond direct care, across public and private healthcare.[6]

Currently in Ireland, there are multiple agencies with responsibility for health information, including the Department of Health, the HSE and HIQA. While there are some governance structures in place for sharing information, there is a need for enhanced governance structures for health information. The eHealth Strategy, published in 2013,[43] called for an independent entity (eHealth Ireland) to be established, outside of the HSE, with a legislative remit to provide strategic leadership and governance to

§§ Sláintecare, published in 2018, is the ten-year programme to transform health and social care services. It is the roadmap for building a world-class health and social care service for the Irish people.

support the collection, use and sharing of health information in Ireland. However, to date, eHealth Ireland has not been formally established as a separate strategic entity to the HSE. HIQA's position paper once again strongly emphasises the significant need for robust strategic leadership and governance for health information, and recommends that eHealth Ireland should be established as "a separate entity with responsibility for overall governance around eHealth implementation — including funding, legal enabling, public awareness and stakeholder engagement through building the eHealth ecosystem in Ireland" and that "the remit of this entity should be broader than eHealth and include the centralised coordination and governance of national data collections and the uses of information beyond direct care at a national level". In an absence of a strategic entity like eHealth Ireland to provide the necessary focus for leadership and governance for health information, there will continue to be an overall lack of accountability and coordination for information across the health and social care system, as well as significant delays in achieving the vision for eHealth as set out in Sláintecare.[6] This is particularly relevant to the implementation of the recommended consent model and to promote the appropriate and effective collection, use and sharing of health information.

National structures for use of information beyond direct care

Robust governance structures are required for the use of information beyond direct care due to the vast amount of data that can be potentially linked and shared. Jurisdictions with specific health information legislation have also outlined detailed governance structures for the use of information beyond direct care. In some jurisdictions, such as in Finland and Australia, specific agencies are assigned responsibility for managing data requests and applying linkage and anonymisation techniques.[45,46] In Finland, Findata was established as the data permit authority and offers a range of services including linking and anonymising data and providing a secure remote access environment. Data security standards are approved by an independent data security assessment body which provides an extra level of protection through this monitoring role. Findata facilitates the effective use of information beyond direct care while safeguarding privacy by operating in a regulated environment that meets data security standards. In Ireland, there is currently no specific agency with the technical infrastructure or responsibility for governance and management of the use of information beyond direct care. The Central Statistics Office (CSO) provides a limited 'trusted third party' and linkage service for researchers, primarily in respect of official statistics and in accordance with strict protocols. However, its capacity to respond to such requests is limited. The consequence of this is that existing health information is not used to its full potential.

In a recent report on secondary use of health data across Europe, in comparison to other European countries, Ireland was ranked as having 'limited vision' in terms of recognising the value of secondary use of health data and using data infrastructure, and as having fragmented practices and strategies that are not fully implemented.[41] Furthermore, results of a survey carried out by the OECD highlighted that Ireland is lacking a central

body to process and make data available in an efficient manner. This has significant implications for the effective and safe use of existing health information. Of the 23 countries that participated in this OECD survey, 17 reported that all of their key healthcare datasets are de-identified prior to analysis. However, Ireland was listed as one of two countries that did not report that data are de-identified prior to analysis of key healthcare datasets.[40] Nineteen participating countries reported that there are standard practices for the treatment of variables that pose a re-identification risk for all, or most, healthcare datasets; Ireland was one of four countries that did not have this capability.[40]

In 2016, the Data Access Storage Sharing and Linkage (DASSL) model was initially proposed as a solution to promote the effective and safe use of health information for research purposes in Ireland.[47] It identified the need for a safe and trusted modern infrastructure that would enable researchers to unlock the significant value of currently underexploited data for the public good. The HRB-funded project, *'Development of a proof of concept data environment for health and related research under the DASSL model'*, examines whether the DASSL model remains international best practice, as technologies and similar models abroad evolve quickly.[48] The project focuses on the technical implementation of infrastructure to support the DASSL model including data controllers, trusted third parties for indexing and linking services, and a safe haven for data analysis. Finally, the project will provide concrete plans of how the proof of concept infrastructure can be scaled-up into an appropriate national system. The learnings from this DASSL project will be important to assess the requirements for a scaled-up model to support the use of health information for reasons beyond direct care, and the necessary governance structure to support such a model (this will be discussed further in Chapter 5).[47]

In other jurisdictions, a specific healthcare agency is assigned with responsibility for governing and managing the use and sharing of information beyond direct care and a national committee is appointed to oversee the use of information beyond direct care. Both of these requirements are absent in Ireland at present and are essential, not only to promote the safe effective use of information, but also to ensure expertise and capabilities are developed in line with international best practice.

Local level structures for information governance

Health and social care services must adhere to the principles of data protection which are set out in the GDPR and the Data Protection Act 2018. In terms of accountability for the management of information, the GDPR sets out the requirements for the designation of a Data Protection Officer for any organisation that processes personal data. The UK, operating in compliance with their Data Protection Act 2018,[49] provides a good practice example of developing a network to support the use and protection of data across health and social care services. As well as the advisory role provided by the National Data Guardian, there is an established network of Caldicott Guardians.[50] A Caldicott Guardian is a senior person responsible for protecting the confidentiality of people's health information and making sure it is used properly. The aim of this network is to assist and guide in developing consistent standards and guidance for information governance and the use of data at a service provision level. The UK Caldicott Guardian Council (UKCGC) is the national body for Caldicott Guardians which is also responsible for encouraging consistent standards and training, as well as developing guidance and policies relating to the Caldicott principles.[51] All NHS organisations and local authorities which provide social services must have a Caldicott Guardian. Caldicott Guardians apply the eight principles [51] to ensure that people's information is kept confidential and used appropriately.

In Ireland, within the HSE, the overall accountability for collection, use and sharing of health information lies with senior and local accountable officers in compliance with the delegation and performance and accountability frameworks. Accountable Officers are fully responsible and accountable for the services they lead and deliver.[52,53] In terms of an established network for data governance for services within health and social care, there is one Data Protection Officer and four Deputy Data Protection Officers within the HSE. These offer support for HSE-funded services. In addition, information governance committees are in place in many health and social care services; however, these structures vary across local services. Enhanced structures to support information governance structures at local and regional level, would promote better data protection at a service provision level, as well as the better use of data. Additional guidance and support would also encourage consistent standards or training in this area across all health and social care services in Ireland.

4.1 Recommendations – governance structures to support new legislation and the consent model for health information

HIQA makes the following recommendations:

Governance structures to support new health information legislation and consent model	
6.	As set out in the eHealth Strategy (2013)[43] and HIQA's recent position paper[6] on the reform of Ireland's national health information system, **eHealth Ireland** should be established as an independent entity with oversight for all aspects of health information. eHealth Ireland should have overall responsibility for governance and for ensuring compliance with the new health information legislation and consent model, including: i. providing strategic leadership to enhance the effective use of information beyond direct care. Specifically, eHealth Ireland should establish new national level governance structures, to include: • implementing the DASSL model for the use of information beyond direct care. This should be expanded beyond research to include information for the management and planning of health and social care services. eHealth Ireland should have responsibility for managing activities such as anonymising and linking data, and creating a safe haven for data sharing at this level. • establishing a 'National Data Governance Board for the use of information beyond direct care'. The Board should be comprised of independent specialists in the area of health information, as well as public and patient representatives. Primarily, this Board would be responsible for overseeing and governing a framework for the use and sharing of data for purposes beyond direct care (see Recommendation 7). ii. Enhancing current information governance structures in place at local and regional levels within health and social care services, by establishing a network to support Data Protection Officers, and others responsible for information governance at a service-provision level. The aim of this network should be to assist and guide in developing consistent standards and guidance for the use of data and information within health and social care services in compliance with the new health information legislation.

Chapter 5 – Technical and operational considerations

To support the effective implementation of the recommended consent model, key technical and operational elements need to be developed, such as the capacity to manage consent preferences and a system to support the use of data beyond direct care, similar to the DASSL model, as explained in Chapter 4.[47]

Capturing and managing consent preferences – Citizen health portal

As discussed in Chapter 2, the consent model for processing health information should follow a rights-based approach. This means that an emphasis is placed on protecting and promoting people's rights and respecting their autonomy, privacy, dignity, and their values, preferences and diversity. As technologies develop and the potential to use and share health information increases, the rights of individuals in relation to their personal information should be openly discussed, as well as the choices they have about this. However, in a complex and dynamic environment, the ability to capture and manage consent choices depends on the technical capacity to enable this. The Sláintecare implementation strategy has outlined an action plan, as part of the implementation of the eHealth Programme, to develop a citizen health portal.[44] Significantly, an online citizen health portal for the Irish health system could provide individuals with access to medical records, appointment scheduling, secure messaging and resources for self-care. Some jurisdictions have also used portals as a means of capturing and managing consent preferences. In some cases, such as in Estonia, the portal allows individuals to easily view who has accessed their records, promoting transparency. Findings from a national public engagement on health information, recently published by HIQA,[2] highlight that:

- people want to be able to access their own information via a citizen health portal as they feel this would empower them to play a role in their own care;
- people want to know who has accessed their records and for what purpose;
- many people would like to be able to control who can see certain types of information that are considered more sensitive, for example information about mental health.

The approaches taken by jurisdictions differ in respect to the degree to which individuals have control over the use and sharing of the information contained within an EHR. In developing portals, some jurisdictions have provided a significant degree of control to individuals in both the initiation of the account on the portal and the level of control thereafter. In some cases, individuals also have a significant level of control over their own information by limiting who has access to their record, as well as blocking and removing access to certain information or documents for direct care. There has also been a trend towards making it easy for individuals to review and decide how they want their information to be used and shared for reasons beyond direct care.

The approach taken in Australia in the development of My Health Record provides the individual with the highest degree of control, where individuals can choose to opt-out of having a My Health Record at any time through the portal.[23] When an individual cancels a My Health Record, all information in the record, including any backups, is permanently deleted from the system.[54] Deleted information cannot be recovered so it is no longer available to the individual or their healthcare providers, including in an emergency. In Finland, consent to creating an EHR is provided by the patient by signing a specific consent form or via an electronic portal (*MyKanta*). Once an individual consents to having an EHR created and the healthcare unit in question has started using the repository, an individual no longer can choose to opt-out of the information from their record being stored in the national patient data repository.[14] In such instances, individuals are informed that by not having an EHR, it may impact on their direct care as healthcare professionals may not be able to make fully-informed decisions.

Recent evidence shows that some jurisdictions are moving away from an opt-out model for the initiation of eHealth initiatives, on safety grounds, and moving towards a model that gives individuals greater control of information within their records.[29,30] Examples of greater control for use of information for direct care and for uses of information beyond direct care were discussed in Chapter 2 under consent preferences; the level of detail at which preferences can be specified depends on the technical capability within the portals. In Australia, Estonia, Finland and Ontario (Canada), individuals can limit access to their information by restricting access to data in the EHR using different approaches. In Australia, a Record Access Code (RAC) can be used to allow only specific healthcare professionals to access their My Health Record and certain records can also be blocked. Similarly, in Ontario (Canada), a consent directive can be added to the electronic record which allows the individual to specify that certain information should not be accessed without their consent. In Finland, individuals can issue a 'refusal' to access information through the healthcare services or online in My Kanta Pages.[26]

As outlined in Chapter 2, in relation to consent to the use of information beyond direct care, Australia and England have implemented an opt-out model where individuals can opt-out of having their information being used for different purposes. In most jurisdictions included in the evidence review, the infrastructure to enable people to manage or change their consent preferences is delivered through portals, except for England which has a specific online platform, as described previously, in absence of a national citizen health portal.

The specific detail regarding the technology and capability to enable individuals to manage consent preferences, for use of information for direct care and reasons beyond direct care, should be explored through significant engagement with the public (this will be discussed further in Chapter 6).

Effective use of data beyond direct care

As outlined in Chapter 2, individuals' health information can often be de-identified before being used for reasons beyond direct care. In jurisdictions with advanced frameworks for the use of information for reasons beyond direct care, there are specific agencies responsible for management of the information at this level.[45,46] These agencies have a role in managing data requests and have expertise in the latest anonymisation and linkage techniques. When such data governance structures and technical infrastructure are in place, existing data and information can be anonymised and then shared securely ensuring the optimal use of data to inform policy and practice, and to support innovation. In absence of a specific healthcare agency with the infrastructure and capacity to manage such a service, it results in a rudimentary approach to the use of existing health information. To manage this process in a safe and controlled environment, the appropriate infrastructure and expert skillset are required.

As discussed in Chapter 4, the learnings from this DASSL model proof of concept project will be important to assess the requirements for a scaled-up model to support the use of information for reasons beyond direct care, and the necessary governance structures to support such a model. The project focuses on the technical implementation of infrastructure to support the DASSL model, including data controllers, trusted third parties for indexing and linking services, and a safe haven for data analysis. The learnings from this project will be key to deciding the appropriate technical and operational consideration for the use of data beyond direct care in Ireland.

Guidance to support the consent model

As discussed in Chapter 2, it is imperative that everybody working in the health and social care system understands their responsibilities and obligations in relation to the collection, use and sharing of health information. However, in the absence of a legal framework for, and guidance on, the collection, use and sharing of health information, it is difficult for those working in the field to use health information to its full potential and to be confident that they are collecting, using, and sharing information in a way that respects individuals' rights to privacy and confidentiality. Therefore, it is important to provide clarity on obligations and responsibilities for those working in health and social care services. As this is a complex and evolving area, guidance and code of practice would help to develop a common understanding around individuals' rights in relation to health information. In New Zealand and Northern Ireland, legally-mandated codes of practice that govern health information have recently been introduced. For example, in Northern Ireland, the *'Code of Practice on Protecting the Confidentiality of Service User Information',* published in 2019, supports and guides all those involved in health and social care regarding decisions relating to the protection, use and sharing of service user information.[19] Similarly, in 2020, New Zealand published the 'Health Information Privacy Code' which outlines rules for health agencies regarding the collection, use, storage and sharing of health information.[55] Furthermore, in parallel to developing the DASSL

model, to support the effective use of information beyond direct care, detailed guidance would help to outline best practice in relation to anonymisation and linking of health data.

5.1 Recommendations – Technical and operational considerations

HIQA makes the following recommendations:

Technical and operational requirements	
7.	eHealth Ireland, through consultation with stakeholders, including the new 'National Data Governance Board for the use of information beyond direct care', should develop an implementation plan outlining the requirements for the technical infrastructure and operational capabilities necessary to implement the consent model for the collection, use and sharing of health information, taking into account both current and future needs. This plan should include specific details on: ▪ how the health and social care system will manage individuals' consent and control preferences for how personal information is used and shared. ▪ an anomymisation, linkage and secure sharing service for the use of information beyond direct care – DASSL model.
8.	The Department of Health should identify the appropriate organisations with responsibility to develop codes of practice and guidance materials to support the consent model for the collection, use and sharing of health information, as well as the new proposed legislation. As a priority, this should include: ▪ guidance for individuals to explain: the reasons how, and why, personal information is being used; and rights to privacy and maintaining confidentiality of health information, and what choices people have about this. ▪ a Code of Practice on protecting individuals' confidentiality for health and social care professionals. ▪ a Code of Practice to outline best practice in relation to anonymisation*** and linking of health data, and details as to who is authorised to undertake such activates in compliance with the consent model and new health information legislation.

*** Effective anonymisation may not always be possible due to the nature or context of the data or the purpose(s) for which it is collected and used.

Chapter 6 – Public engagement

The collection, use and sharing of personal health information is a very complex and dynamic area as individuals' perceptions, experiences and opinions are constantly evolving. This is happening in the context where technical advances are occurring in terms of how information is collected, used and shared. International evidence has shown that public engagement and involvement is extremely important for the successful introduction of new technologies. Jurisdictions that have implemented successful health information initiatives have undertaken significant and ongoing engagement with the public.[56,57] There are also a number of examples of large scale health information initiatives failing due to poor public engagement. In 2013, England tried to implement a national database of patient interactions with the healthcare system called '*care.data*'. Following three years of debate and controversy, the care.data scheme was closed in 2016.[58] Subsequently, in an attempt to rebuild trust, the Understanding Patient Data organisation was set up to support better conversations about the uses of health information between healthcare providers, government and the public.[30]

Public engagement in relation to the collection, use and sharing of health information is an extremely important element of building a culture of trust. It is an important tool to help understand what level of trust currently exists and what is acceptable to people in relation to their health information. It is also used to inform the public on the benefits of information sharing across the health system so that there is a universal understanding of the need to share information, as well as clearly explaining the steps taken to ensure privacy is maintained and systems are secure. As eHealth initiatives are advanced, the coming years will present huge changes to the way health information is collected, used and shared, and therefore a specific public engagement plan should be developed in the area of health information. This plan needs to thoroughly explore the public's views, opinions and preferences of the new health information legislation as this will be the basis upon how personal information will be processed in health and social care services. In addition, as eHealth plans are developed, the public should be able to trust that their personal health information is used appropriately in ways that are acceptable to them and therefore, public engagement must be undertaken in a meaningful and authentic way to build trust and confidence. This will ensure that new technologies and initiatives, such as EHRs and a citizen portal, are implemented in a way that is acceptable.

There is now strong evidence that the Irish public want to see advances in eHealth initiatives and want to have more control over their health information. In addition to the national public engagement on health information that has informed these recommendations, [2] a recent citizens' jury on access to health information organised by the Irish Platform for Patient Organisations, Science and Industry (IPPOSI) identified that individuals should be the owners of their own health data and that practices, processes, and policies developed to manage or share health information must be made in partnership with them.[59]

Currently, there is much debate about the advantages and disadvantages of opt-out models for the initiation of EHRs and for the uses of health information beyond direct care. Opt-out models are based on the principle that providing people with a mechanism to opt-out shows that their autonomy is being respected; upholding the choices that people make is vital for demonstrating trustworthiness.[60] While this is an important mechanism to build trust, it is also important to note that although opt-out models of consent are being used in a number of jurisdictions, this approach is also associated with some disadvantages. For example, if large numbers of people have concerns and choose to opt-out of their information being used for reasons beyond direct care, the information will no longer be representative of the entire population and may not give an accurate reflection of the current situation. This would cause significant issues when using this information to inform decision-making, in particular, for planning or management of services.[60] In addition, this approach is thought to disadvantage certain individuals, such as those with poor health literacy or those facing other language and technological barriers, as they may be unable to take the steps necessary to opt-out.[61] Similarly, it should also be noted that providing people with the opportunity to opt-out of having an EHR may be associated with a patient safety risk as, if a person opts-out, their health information will not be available to clinicians at the point-of care. This has the potential to result in sub-optimal decision-making, particularly during emergencies.[29] As such, it is important that countries take into account multiple factors and perspectives when deciding on what consent approach to take when implementing EHRs, or other significant eHealth initiatives or changes. In Ireland, this highlights the need for adequate public engagement to be undertaken before any new technologies or systems are implemented in order to ensure they are implemented in a way that is acceptable to the public, including disadvantaged groups, and also to establish and maintain public trust.

Involving people in important decisions about their health information and ensuring that their rights in relation to health information are upheld is crucial as systems evolve and practices change. From the international literature, public engagement is carried out for a variety of reasons, depending on the maturity of the engagement levels, including: informing the public of a new initiative or the benefits of sharing in a controlled manner; consulting to understand the knowledge, experiences and preferences regarding the collection, use and sharing of health information; and collaborating to achieve a deeper understanding of preferences and needs.[4] A strategic plan for public engagement in the area of health information should be developed based on the International Association for Public Participation (IAP2)[62] framework, and should build on the collaboration between HIQA, the Department of Health and the HSE in undertaking the first national public engagement on health information.[2] The importance of public engagement has also been acknowledged in the Sláintecare Implementation Strategy and Action Plan 2021-2023.[44] One of the core principles set out in the Sláintecare plan is to effectively engage with the public to build confidence in the health system and a commitment has

been made to launch a comprehensive public engagement plan.

6.1 Recommendations – Public engagement

HIQA makes the following recommendations:

Public engagement	
9.	In order to build and maintain trust with the public, there must be transparency and ongoing engagement to ensure individuals can appropriately participate in decision-making about how their health information is being collected, used and shared.
10.	Using a partnership model, the Department of Health, the HSE and HIQA should develop a **national public engagement strategy** for health information to inform, consult, involve, collaborate with and empower[†††] citizens, and health and social care professionals, to make decisions on proposed changes and ongoing initiatives which impact on how health information is collected, used and shared. The strategy should detail a system-wide approach to actively informing individuals about how their personal information is used, and what individuals' rights are in relation to privacy and maintaining confidentiality. Public engagement should be undertaken to establish preferences and opinions on: ▪ the new health information legislation ▪ the consent process, including considerations on an 'opt-out model' ▪ new eHealth initiatives ▪ any significant changes to how health information is collected, used and shared.

[†††] Based on the framework for public participation developed by the International Association for Public Participation.

Chapter 7 – Conclusion and next steps

A consent model is required to clearly outline the situations when consent is, and is not, required for the use of personal information in health and social care. Sharing personal information in a secure and controlled manner is an integral part of care provision. Health information is invaluable both for managing direct patient care and also for reasons beyond direct care, such as health service planning and management, policy-making and research. Therefore, it is essential that there is a consent model put in place to ensure individuals can consent to the use of their health information for their direct care and for reasons beyond their direct care. However, to support the consent model and to deliver the appropriate legislative requirements and governance structures, a strategic approach is needed to ensure that personal information is processed safely and securely in line with individuals' preferences. This includes the establishment the technical and operational capabilities to support a consent model, as well as significant public engagement in this area.

A recent position paper published by HIQA called for the reform of Ireland's national health information system.[6] It highlighted that over the past 20 years in Ireland, several strategies were published in this area, including the first national health information strategy in 2004,[42] and Ireland's first eHealth strategy in 2013.[43] Many objectives that were set out in these strategies have still not been achieved. The paper recommended developing a health information strategy that takes a holistic and cohesive approach to managing health information, that is, how health information is collected, used and shared for direct care and also for the use of information beyond direct care, across public and private healthcare.[6] In addition, recent international reports have highlighted that Ireland is falling behind in comparison to other EU and OECD countries in terms of health information infrastructure and governance, fragmented practices, and limited capabilities for using health information beyond direct care.[6,40,41] Results of a survey carried out by the OECD, as well as HIQA's position paper, identified that Ireland is lacking a central body to process and make data available in an efficient manner, and that it has significant shortcomings in terms of the use of personal health data.[6,40]

Furthermore, in Ireland, there is a need for a clear legislative framework for the use of health information. The current legislation for health information is complex and not fit-for-purpose, drawing on a number of discrete pieces of legislation making it difficult to understand and navigate. The approaches to developing legislation for health information differs across the international jurisdictions reviewed. However, the decision to develop specific legislation or codes of practice to regulate the collection, use and sharing of health information — for example by Australia, Finland, New Zealand, Northern Ireland and Ontario (Canada) — identifies a clear need to define rules and governance structures for processing health information. When a legislative framework is available, including clear guidance on the rules for processing health information, professionals have the knowledge and confidence to share confidential information in the

best interest of patients and public, and advanced governance structures and appropriate infrastructure are required to ensure that existing information sources can be used to their full potential.

Finally, successful implementation of these initiatives will only be realised with the support, confidence and trust of the public. Involving people in important decisions about their health information and ensuring that their rights in relation to health information are upheld is crucial, and will ensure that new technologies and initiatives are implemented in a way that is acceptable. Public engagement must be undertaken in a meaningful and authentic way to build trust and confidence. As systems evolve and practices are constantly changing, ongoing engagement is necessary to monitor and evaluate the public's views and opinions in this area.

The draft recommendations on a consent model for the collection, use and sharing of health information include the following: defining a number of key concepts linked to the consent model including health information, the use of information for direct care and the use of information beyond direct care; the circumstances when consent is, and is not, required from individuals for the collection, use and sharing of their information; the legislative requirements; the governance structures necessary to ensure that personal information is processed safely and securely in line with individuals' preferences; the technical and operational considerations to support such a consent model; and the requirements for effective public engagement in this area.

Following the public consultation, the draft recommendations will be reviewed and amended to reflect the findings. The updated recommendations will then be circulated to relevant stakeholders, including the Advisory Group for final considerations. Following analysis and review of the additional feedback, the final recommendations document will be completed and sent for approval to the HIQA Executive Management Team, before final approval by HIQA's SIRT Committee (Board subcommittee) and the HIQA Board. After the HIQA Board has approved the recommendations, they will be submitted to the Minister for Health and will also be published on the HIQA website.

Summary of recommendations

Definitions	
1.	Based on a review of international best practice and stakeholder consultation, HIQA recommends that the following terms are defined in legislation: **Health information** is "information[‡‡‡] which relates to the physical or mental health or condition of an individual; the health or social care that is being, has been, or may be provided to an individual, or an individual's expressed wishes about the future provision of health or social care; and other personal information required for the provision of health or social care". The use of **health information for direct care** is "information used to inform the provision of direct care to an individual; activities that focus on improving direct care and are undertaken by health and social care professionals with a legitimate care relationship,[§§§] such as case reviews and local clinical audit; and emergency situations where information use is necessary to lessen or prevent a threat to an individual's life, health or safety". The use of **health information beyond direct care**[****] is "information used and shared by health services and health service providers for activities that contribute to the overall provision of health and social care to a population as a whole, or a group of individuals with a particular condition, but which fall outside the scope of direct care. Uses beyond direct care include: health services management and planning, health and social care research, public health, statistics, and training and education."
Rights-based approach to implementing a consent model	
2.	The collection, use, and sharing of personal information should follow a **rights-based approach.** In all circumstances, individuals should be informed of: ▪ how, and why, their personal information is being, or may be, collected, used and shared. ▪ their rights to privacy and confidentiality in relation to their personal information, and what choices they have about this. To support a rights-based approach, it is important that everybody working in the health and social care system understands their responsibilities and obligations in relation to the collection, use and sharing of personal information. In addition, a system-wide approach is needed to actively inform

[‡‡‡] Information sources includes a wide variety of material, including but not limited to: handwritten notes; electronic records; correspondence, including oral correspondence, between health and social care professionals; visual and audio recordings; laboratory report; and communication with patients and services users (including oral communication, texts and emails).
[§§§] A legitimate care relationship is one where a health and social care professional is involved in informing and delivering the direct care of an individual.
[****] Explicit consent is required for the use of personal information for reasons beyond direct care (except where exemptions apply). Anonymised or aggregated data should be used when the purpose of use can be achieved without personal information, even when exemptions apply.

	individuals about how their personal information is used and what individual's rights are in relation to privacy and maintaining confidentiality (see recommendation 10).
Consent Model	
3.	Based on a review of international evidence, HIQA recommends the introduction of the following consent model for the collection, use and sharing of personal information, and that this model should be defined in legislation (see recommendation 4): **Note**: As a general principle, anonymised or aggregate data should be used in all circumstances where the purpose of use can be achieved without personal information. **Use of information for direct care** ▪ **Category 1:** Explicit consent is not required for direct care. The collection, use and sharing of personal information is lawful under the Data Protection Act 2018 [34] and the General Data Protection Regulation (GDPR)[3] where it is necessary for the provision of health and social care. This means that professionals with a care relationship can collect, use and share personal information to ensure they have accurate and timely information to deliver safe and effective care. However, the principles of data protection and transparency still apply, so individuals should always be fully informed of how, and why, their personal information is being or may be used. **Use of information beyond direct care** ▪ **Category 2:** Explicit consent is required for the collection, use and sharing of personal information for reasons beyond direct care (except where exemptions apply – see Category 3).†††† ▪ **Category 3:** Explicit consent is not required for the collection, use and sharing of personal information if the use is considered one of the following exemptions, as defined below: ➢ **Identification, prevention, control, and surveillance of population health and disease**: The use of information to support the identification, prevention, control and surveillance of population health and disease, including both communicable and non-communicable diseases. ➢ **Compilation or analysis of statistics relevant to health and social care**: The collection, compilation, analysis or interpretation of data, expressed in either numerical or non-numerical form, relevant to health and social care.

†††† In limited situations, when the public interest of doing research significantly outweighs the need for explicit consent, the Health Research Consent Declaration Committee (HRCDC) will review applications and make a final decision on the need for consent. Research Consent Declarations are covered within the Health Research Regulations and therefore are **outside of the scope of these recommendations**.

	➢ **Management and planning of health and social care services:** The use of information to inform the planning, monitoring, delivery, improvement, auditing and evaluation of health services. ➢ **Health and social care professional education and training:** The use of information to develop resource materials or the sharing of information during structured professional development activities in order to support the education and training of health and social care professionals. ➢ **Alternative legislative basis for the collection, use and sharing of personal information:** The collection, use and sharing of personal information is required by law. ○ Each exemption should be clearly defined in legislation and the permitted uses of data within each exemption should be described in supporting regulations and guidance. ▪ **Category 4:** Explicit consent is not required for the sharing of health information if the information is considered anonymised in accordance with the Data Protection Commission's 'Guidance on Anonymisation and Pseudonymisation'.(8) As advances are made in this area, there is a need to ensure that this processing occurs in a regulated and controlled environment with the appropriate governance and infrastructure in place (see recommendations 6 and 7). To support best practice, it is recommended that a code of practice is developed (see recommendation 8).
Legislation	
4.	Building on the data protection principles outlined in GDPR‡‡‡‡ and in line with HIQA's recommendation in the position paper for a legislative framework in the area of health information,(6) the Department of Health should develop specific legislation in relation to the collection, use and sharing of personal information. The legislation should: ▪ incorporate the recommended definitions and proposed consent model, and promote a rights-based approach to the use and sharing of personal information (see recommendations 1-3), ▪ outline how the consent model should be monitored and regulated, addressing current arrangements and future requirements.
5.	To complement new health information legislation, a legislative framework should be developed with supporting regulations, codes of practice and policies. These supporting documents should help to define what good practice is for those working in health and social care services and to develop a common understanding around individuals' rights in relation to health information (see recommendation 8).
Governance structures to support new health information legislation and consent model	
6.	As set out in the eHealth Strategy (2013)(43) and HIQA's recent position paper(6) on the reform of Ireland's national health information system,

‡‡‡‡ The seven data protection principles include: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability.

	eHealth Ireland should be established as an independent entity with oversight for all aspects of health information.[§§§§] eHealth Ireland should have overall responsibility for governance and for ensuring compliance with the new health information legislation and consent model, including: i. providing strategic leadership to enhance the effective use of information beyond direct care. Specifically, eHealth Ireland should establish new national level governance structures, to include: • implementing the DASSL model for the use of data beyond direct care. This should be expanded beyond research to include information for the management and planning of health and social care services. eHealth Ireland should have responsibility for managing activities such as anonymising and linking data, and creating a safe haven for data sharing at this level. • establishing a 'National Data Governance Board for the use of information beyond direct care'. The Board should be comprised of independent specialists in the area of health information, as well as public and patient representatives. Primarily, this Board would be responsible for overseeing and governing a framework for the use and sharing of data for purposes beyond direct care (see Recommendation 7). ii. Enhancing current information governance structures in place at local and regional levels within health and social care services, by establishing a network to support Data Protection Officers, and others responsible for information governance at a service-provision level. The aim of this network should be to assist and guide in developing consistent standards and guidance for the use of data and information within health and social care services in compliance with the new health information legislation.
Technical and operational requirements	
7.	eHealth Ireland, through consultation with stakeholders, including the new 'National Data Governance Board for the use of information beyond direct care', should develop an implementation plan outlining the requirements for the technical infrastructure and operational capabilities necessary to implement the consent model for the collection, use and sharing of personal information, taking into account both current and future needs. This plan should include specific details on: ▪ how the health and social care system will manage individuals' consent and control preferences for how personal information is used and shared.

[§§§§] HIQA's recent publication '*The need to reform Ireland's national health information system to support the delivery of health and social care services*' identified a need for an entity to provide strategic leadership and governance for health information in Ireland. The eHealth Strategy (2013) originally called for a single entity (eHealth Ireland) with responsibility for overall governance around eHealth implementation — including funding, legal enabling, public awareness and stakeholder engagement through building the eHealth ecosystem in Ireland — to work in partnership with Government and state agencies. To date, eHealth Ireland has not been formally established as a separate entity to the HSE. In an absence of an entity like eHealth Ireland, there has been and will continue to be an overall lack of accountability and coordination for information across the health and social care system.

	▪ an anomymisation, linkage and secure sharing service for the use of information beyond direct care – DASSL model.
8.	The Department of Health should identify the appropriate organisations with responsibility to develop codes of practice and guidance materials to support the consent model for the collection, use and sharing of health information and new legislation in this area. As a priority, this should include: ▪ guidance for individuals to explain: the reasons how, and why, personal information is being used; and rights to privacy and maintaining confidentiality of health information, and what choices people have about this. ▪ a Code of Practice on protecting individuals' confidentiality for health and social care professionals. ▪ a Code of Practice to outline best practice in relation to anonymisation***** and linking of health data, and details as to who is authorised to undertake such activates in compliance with the consent model and new health information legislation.
Public engagement	
9.	In order to build and maintain trust with the public, there must be transparency and ongoing engagement to ensure individuals can appropriately participate in decision-making about how their personal information is being collected, used and shared.
10.	Using a partnership model, the Department of Health, the HSE and HIQA should develop a **national public engagement strategy** for health information to inform, consult, involve, collaborate with and empower††††† citizens, and health and social care professionals, to make decisions on proposed changes and ongoing initiatives which impact on how health information is collected, used and shared. The strategy should detail a system-wide approach to actively informing individuals about how their personal information is used, and what individuals' rights are in relation to privacy and maintaining confidentiality. Public engagement should be undertaken to establish preferences and opinions on: ▪ the new health information legislation ▪ the consent process, including considerations on an 'opt-out model' ▪ new eHealth initiatives ▪ any significant changes to how health information is collected, used and shared.

***** Effective anonymisation may not always be possible due to the nature or context of the data or the purpose(s) for which it is collected and used.
††††† Based on the framework for public participation developed by the International Association for Public Participation.

Glossary of terms

Anonymisation: Processing of data or information with the aim of irreversibly preventing the identification of the individual to whom it relates. Data or information can be considered effectively and sufficiently anonymised if it does not relate to an identified or identifiable natural person or where it has been rendered anonymous in such a manner that the data subject is not or no longer identifiable.

Aggregate data: data that have been summed and/or categorised to a level that ensures the identities of individuals or organisations cannot be determined by a reasonably foreseeable method.

Case Reviews: the process of examining and reporting on an individual's treatment and care history. Cases are typically reviewed by the treating medical team.

Citizen health portal: A health portal, or patient portal as described in some jurisdictions, is specially created to allow online access for individuals to their own healthcare information through apps on their smartphone or other devices, or using a website. In many countries, patients use a portal to access to their EHR, where they can see their latest test results, clinical correspondence, request repeat medications and to request appointments. Some portals also enable patients to add their own health information, to maintain their own record of home monitoring for conditions such as diabetes. In another example, the record may provide a parent with the ability to add supplementary entries to an incomplete vaccination record for their child. The clinician reviewing the record can then review these and the original entries to gain a better understanding of the child's vaccination history.

Clinical Audit: a clinically-led quality improvement process that seeks to improve patient care and outcomes through systematic review of care against explicit criteria, and acting to improve care when standards are not met. The process involves the selection of aspects of the structure, processes and outcomes of care which are then systematically evaluated against explicit criteria. If required, improvements should be implemented at an individual, team or organisation level and then the care re-evaluated to confirm improvements.

Data: facts and statistics and individual detail are considered data. Data can be described as numbers, symbols, words, images and graphics that have been validated but are yet to be organised or analysed.

Data linkage: a method of bringing information from different sources together about the same person or entity to create a new, richer dataset.

De-identification: Processing of data or information so that there is a reduced likelihood of an individual being reasonably identified, although re-identification may be possible through deliberate techniques, such as linkage with other sources.

eHealth: eHealth enables health information to be managed in a coordinated way. The World Health Organization (WHO) defines eHealth as 'the cost-effective and secure use of information and communications technologies in support of health and health-related field, including health care services, health surveillance, health literature, and health education, knowledge and research'.

ePrescribing: ePrescribing can be described as a three-step approach. First, at the time of prescribing medications for a patient, the prescriber's clinical information system generates the prescription in electronic format. Second, the electronic format of the prescription is transmitted to a message exchange or mailbox and, when the patient presents in a pharmacy requesting their medication, the pharmacist retrieves the electronic prescription from the message exchange. Third, the pharmacists dispenses the medication and reports on the medicines given to the patient.

Health and social care: activities that focus on the preservation or improvement of the health or wellbeing of others; the diagnosis, treatment or care of those who are injured, sick, disabled or infirm; the resolution, through guidance, counselling or otherwise, of personal, social or psychological problems; the care of those in need of protection, guidance or support.

Health and Social Care Professional: A health or social care professional is any person that exercises skill or judgment relating to any activity included in the definition of health and social care.

Health and social care research: research designed and conducted to generate new generalisable or transferrable knowledge that could lead to changes to treatments, policies or care in relation to health and social care. As defined in the Health Research Regulations 2018, health research is:

- research with the goal of understanding normal and abnormal functioning, at the molecular, cellular, organ system and whole body levels;
- research that is specifically concerned with innovative strategies, devices, products or services for the diagnosis, treatment or prevention of human disease or injury;
- research with the goal of improving the diagnosis and treatment (including the rehabilitation and palliation) of human disease and injury and of improving the health and quality of life of individuals;
- research with the goal of improving the efficiency and effectiveness of health professionals and the health care system;
- research with the goal of improving the health of the population as a whole or any part of the population through a better understanding of the ways in which social, cultural, environmental, occupational and economic factors determine health status.

Health information system: Throughout the literature, the term 'health information system' varies, often with no clear or precise definition and has become an umbrella term encompassing a number of systems — both electronic and paper-based — for capturing and transferring health information. For the purpose of this paper, a health information system encompasses all health information sources required by a country to plan and implement its national health strategy. Examples of these data sources are EHRs, surveillance data, census data, population surveys, and national health and social care data collections.

Identifiable data: data that identifies an individual or for which it is reasonably foreseeable in the circumstances that it could be utilised, either alone or with other information/data, to identify an individual.

Information: When data are processed, interpreted, organised, analysed, structured or presented so as to make them meaningful or useful, they are then information.

National electronic health records (EHRs): is a complete digital record of a patient's journey, throughout their life, across all health and social care settings, for every citizen. An EHR contains the information documented by healthcare professionals when they interact with that patient — for example, the patient's symptom history, past history of illnesses and operations, clinical observations made by the professional such as a blood pressure reading, blood and other test results, X-rays and scan results, prescriptions and other treatments, care advice, the course of the illness, preventive and public health activities such as immunisations, and activities undertaken by patients to stay healthy. An EHR system can support healthcare professionals by facilitating, for example, the use of checklists, alerts, and predictive tools, and embedding clinical guidelines, electronic prescribing and the ordering of tests.

Personal data or information: any data or information relating to an identified or identifiable individual. An identifiable individual is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.

Pseudonymsation: Processing of personal data or information in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, provided that— (a) such additional information is kept separately from the data, and (b) is subject to technical and organisational measures to ensure that the data are not attributed to an identified or identifiable individual.

Safe haven: an environment in which data are held securely and where access to data is highly controlled and restricted. Under agreed processes, health data may be processed and linked with other health data (and/or non-health related data) and made

available in a de-identified form for reasons beyond direct care. Safe havens may be developed as on-site facilities or provided through remote access solutions, as long as privacy standards can be equally maintained.

Glossary of abbreviations

Abbreviation	Definition
AIHW	Australian Institute of Health and Welfare
CIDR	Computerised Infectious Disease Reporting
CSO	Central Statistics Office
DASSL	Data Access Storage Sharing and Linkage
EHR	Electronic Health Record
EU	European Union
GDPR	General Data Protection Legislation
HIQA	Health Information and Quality Authority
HRCDC	Health Research Consent Declaration Committee
HSE	Health Service Executive
NHS	National Health Service
ICT	Information and Communications Technology
IPPOSI	Irish Platform for Patient Organisations, Science and Industry
OECD	Organisation for Economic Co-operation and Development
PAS	Patient Administration System
PCRS	Primary Care Reimbursement Service
RAC	Record Access Code
SIRT	Standards Information Research and Technology
UKCGC	United Kingdom Caldicott Guardian Council

References

1. Health Act 2007 (Ireland). Available from: https://www.irishstatutebook.ie/eli/2007/act/23/enacted/en/html. Accessed on: 28 October 2021.

2. Health Information and Quality Authority, Department of Health, Health Service Executive. *Findings from the National Public Engagement on Health Information 2020 - 2021*. Dublin: 2021. Available from: https://www.hiqa.ie/sites/default/files/2021-09/Findings-from-the-National-Public-Engagement-on-Health-Information.pdf. Accessed on: 28 October 2021.

3. General Data Protection Legislation 2016 (European Union). Available from: https://gdpr-info.eu/. Accessed on: 28 October 2021.

4. Health Information and Quality Authority. *Evidence Synthesis: Recommendations for a consent model on the collection, use and sharing of health information*. Dublin: 2021. Accessed on: 22 November 2021.

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

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

7. Irish Government Department of Health. *National Clinical Guidelines* [Online]. Available from https://www.gov.ie/en/collection/c9fa9a-national-clinical-guidelines/. Accessed on: 28 October 2021.

8. Data Protection Commission. *Guidance Note: Guidance on Anonymisation and Pseudonymisation*. 2019. Available from: https://www.dataprotection.ie/sites/default/files/uploads/2020-09/190614%20Anonymisation%20and%20Pseudonymisation.pdf. Accessed on: 28 October 2021.

9. The National Data Guardian. *Review of Data Security, Consent and Opt-Outs*. London: 2016. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/535024/data-security-review.PDF. Accessed on: 28 October 2021.

10. Health Information and Quality Authority, Safeguarding Ireland. *Guidance on a Human Rights-based Approach in Health and Social Care Services* Dublin: 2019. Available from: https://www.hiqa.ie/sites/default/files/2019-11/Human-Rights-Based-Approach-

Guide.PDF. Accessed on: 1 November 2021.

11. Health Services Organization Act 2001 (Estonia). Available from: https://www.riigiteataja.ee/en/eli/508012018001/consolide. Accessed on: 29 October 2021.

12. Personal Data Protection Act 2018 (Estonia). Available from: https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/523012019001/consolide. Accessed on: 29 October 2021.

13. Health Information Privacy Code 2020 (New Zealand). Available from: https://www.privacy.org.nz/assets/Codes-of-Practice-2020/Health-Information-Privacy-Code-2020-website-version.pdf. Accessed on: 29 October 2021.

14. Secondary Use of Health and Social Data Act 2019 (Finland). Available from: https://stm.fi/en/secondary-use-of-health-and-social-data. Accessed on: 29 October 2021.

15. Health and Social Care (National Data Guardian) Act 2018 (United Kingdom). Available from: https://www.legislation.gov.uk/ukpga/2018/31/contents/enacted. Accessed on: 29 October 2021.

16. Health and Social Care (Control of Data Processing) Act (Northern Ireland) 2016 (Northern Ireland). Available from: https://www.legislation.gov.uk/nia/2016/12/notes. Accessed on: 29 October 2021.

17. Data Protection Act 2018 (Finland). Available from: https://www.finlex.fi/en/laki/kaannokset/2018/en20181050.pdf. Accessed on: 2 November 2021.

18. The Personal Information Protection and Electronic Documents Act 2000 (Canada). Available from: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda. Accessed on: 3 November 2021.

19. Northern Ireland Department of Health. *Code of Practice on Protecting the Confidentiality of Service User Information*. 2019. Available from: https://www.health-ni.gov.uk/sites/default/files/publications/health/user-info-code2019.pdf. Accessed on: 29 October 2021.

20. European Commission. *EU Charter of Fundamental Rights* [Online]. Available from https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights_en. Accessed on: 28 October 2021.

21. Data Protection Commission. *Data protection – not an absolute right* [Online]. Available from https://www.dataprotection.ie/en/dpc-guidance/blogs/data-protection-

not-absolute
right#:~:text=Data%20protection%20%E2%80%93%20not%20an%20absolute%20right%2008th,protection%20of%20personal%20data%20concerning%20him%20or%20her. Accessed on: 28 October 2021.

22. Prictor, M., Lewis, M. A., Newson, A. J., Haas, M., Baba, S., Kim, H., et al. Dynamic Consent: An Evaluation and Reporting Framework. *Journal of Empirical Research on Human Research Ethics*. 2020; 15(3):[175-86 pp.].

23. Australian Digital Health Agency. *My Health Record* [Online]. Available from https://www.myhealthrecord.gov.au/for-you-your-family. Accessed on: 28 October 2021.

24. Personal Health Information Protection Act 2004 (Canada). Available from: https://www.canlii.org/en/on/laws/stat/so-2004-c-3-sch-a/latest/so-2004-c-3-sch-a.html. Accessed on: 29 October 2021.

25. Milieu Ltd. *Overview of the national laws on electronic health records in the EU Member States - National Report for the Republic of Estonia*. 2014. Available from: https://ec.europa.eu/health/sites/default/files/ehealth/docs/laws_estonia_en.pdf. Accessed on: 1 November 2021.

26. Australian Digital Health Agency. *Set an access code on your record* [Online]. Available from https://www.myhealthrecord.gov.au/for-you-your-family/howtos/set-access-code. Accessed on: 29 October 2021.

27. Bragge, P., Bain, C. *Opting out of My Health Records? Here's what you get with the status quo* [Online]. Available from https://theconversation.com/opting-out-of-my-health-records-heres-what-you-get-with-the-status-quo-100368. Accessed on: 2 November 2021.

28. Kemp K, Baer Arnold, B., Vaile, D. *My Health Record: the case for opting out* [Online]. Available from https://theconversation.com/my-health-record-the-case-for-opting-out-99302. Accessed on: 2 November 2021.

29. Privacy Advisory Committee. *Meeting Minutes - 57th Meeting of the Privacy Advisory Committee - Wednesday, 21st January 2021*. 2021. Available from: http://www.privacyadvisorycommittee.hscni.net/PAC_57th%20Meeting_21%20January%202021_Minutes.pdf Accessed on: 2 November 2021.

30. Health Information and Quality Authority. *International review of consent models for the collection, use and sharing of health information*. Dublin: 2020. Available from: https://www.hiqa.ie/sites/default/files/2020-02/International-Review%E2%80%93consent-models-for-health-information.pdf. Accessed on: 28 October 2021.

31. United States Departmet of Health and Human Services. *Advantages of Electronic*

Health Records [Online]. Available from https://www.healthit.gov/faq/what-are-advantages-electronic-health-records#:~:text=Advantages%20of%20Electronic%20Health%20Records%20EHR%20s%20and,for%20patients%20and%20provide%20better%20health%20care%20by%3A. Accessed on: 11 November 2021.

32. NHS Digital. *Choose if data from your health records is shared for research and planning* [Online]. Available from https://www.nhs.uk/your-nhs-data-matters/where-your-choice-does-not-apply/. Accessed on: 29 October 2021.

33. Australian Digital Health Agency. *Choose how your data is used for research* [Online]. Available from https://www.myhealthrecord.gov.au/for-you-your-family/howtos/choose-how-your-data-is-used-for-research. Accessed on: 29 October 2021.

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

35. Health and Social Care Act 2012 (England). Available from: https://www.legislation.gov.uk/ukpga/2012/7/contents/enacted. Accessed on: 29 October 2021.

36. My Health Records Act 2012 (Australia). Available from: https://www.legislation.gov.au/Details/C2017C00313. Accessed on: 28 October 2021.

37. The Health Act 2005 (Denmark). Available from: http://www.ilo.org/dyn/natlex/natlex4.detail?p_isn=70825. Accessed on: 28 October 2021.

38. The Ministry of Health. *Healthcare in Denmark - An Overview*. Denmark: 2016. Available from: https://www.digitalhealthnews.eu/images/stories/pdf/healthcare_in_denmark.pdf. Accessed on: 28 October 2021.

39. Canada Health Infoway. *EHRS Blueprint – an interoperable EHR framework.* 2006. Available from: https://www.infoway-inforoute.ca/en/component/edocman/391-ehrs-blueprint-v2-full/view-document?Itemid=0. Accessed on: 28 October 2021.

40. Oderkink, J. *OECD Health Working Papers No.127 - Survey Results: National health data infrastructure and governance*. 2021. Available from: https://www.oecd-ilibrary.org/docserver/55d24b5d-en.pdf?expires=1635850631&id=id&accname=guest&checksum=CE5C7CA6A1CFCCA3DF577F521A7810D4. Accessed on: 2 November 2021.

41. Open Data Institute. *Secondary use of health data in Europe*. 2021. Available

from: http://theodi.org/wp-content/uploads/2021/09/Secondary-use-of-Health-Data-In-Europe-ODI-Roche-Report-2021-5.pdf. Accessed on: 2 November 2021.

42. Department of Health and Children. *Health Information - A National Strategy*. Dublin: 2004. Available from: https://www.icgp.ie/speck/properties/asset/asset.cfm?type=LibraryAsset&id=04541D6E%2DA15A%2DD1AE%2D76107A995DD4A7D3&property=asset&revision=tip&disposition=attachment&app=icgp&filename=DOHC%5Fhealth%5Finformation%5Fstrategy%2Epdf . Accessed on: 28 October 2021.

43. Irish Government Department of Health. *eHealth Strategy for Ireland*. Dublin: 2013. Available from: https://assets.gov.ie/16174/092e7c62f97b472b83cdb6dfdcdfd5c7.pdf. Accessed on: 28 October 2021.

44. Irish Government Department of Health. *Sláintecare Implementation Strategy and Action Plan 2021-2023*. Dublin: 2021. Available from: https://www.gov.ie/en/publication/6996b-slaintecare-implementation-strategy-and-action-plan-2021-2023/. Accessed on: 28 October 2021.

45. Australian Institute of Health and Welfare. *Data Linkage* [Online]. Available from https://www.aihw.gov.au/our-services/data-linkage. Accessed on: 28 October 2021.

46. Findata. *Findata - The Finnish Social and Health Data Permit Authority* [Online]. Available from https://findata.fi/en/. Accessed on: 28 October 2021.

47. Moran, R. *Proposals for an Enabling Data Environment for Health and Related Research in Ireland - A discussion document*. Dublin: 2016. Available from: https://www.hrb.ie/fileadmin/publications_files/Proposals_for_an_Enabling_Data_Environment_for_Health_and_Related_Research_in_Ireland.pdf. Accessed.

48. Health Research Board. *Proof of Concept technical model for 'DASSL' (Data Access, Storage, Sharing and Linkage) award 2019 (Closed)* [Online]. Available from https://www.hrb.ie/funding/funding-schemes/all-funding-schemes/grant/proof-of-concept-technical-model-for-dassl-data-access-storage-sharing-and-linkage-award-2019/. Accessed on: 2 November 2021.

49. Data Protection Act 2018 (United Kingdom). Available from: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted. Accessed on: 28 October 2021.

50. United Kingdom Government. *UK Caldicott Guardian Council* [Online]. Available from https://www.gov.uk/government/groups/uk-caldicott-guardian-council. Accessed on: 28 October 2021.

51. The National Data Guardian. *The Eight Caldicott Principles*. London: 2020.

Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/942217/Eight_Caldicott_Principles_08.12.20.pdf. Accessed on: 28 October 2021.

52. Health Service Executive. *Performance and Accountability Framework*. Dublin: 2020. Available from: https://www.hse.ie/eng/services/publications/serviceplans/service-plan-2020/performance-and-accountability-framework-2020.pdf#:~:text=The%20objective%20of%20the%20Performance%20and%20Accountability%20Framework,context%20%E2%80%98Accountability%20is%20about%20delivering%20on%20a%20commitment. Accessed on: 29 October 2021.

53. National Delegations Office, Health Service Executive. *Delegation Policy Framework and Governance Arrangements version 5*. Limerick: 2015. Available from: https://www.hse.ie/eng/about/who/delegations-office/delegation-framework-and-government-arrangements.pdf. Accessed on: 29 October 2021.

54. Australian Digital Health Agency. *Cancel a My Health Record* [Online]. Available from https://www.myhealthrecord.gov.au/for-you-your-family/howtos/cancel-my-record. Accessed on: 1 November 2021.

55. New Zealand Office of the Privacy Commissioner. *Health Information Privacy Code*. Wellington: 2020. Available from: https://www.privacy.org.nz/assets/Codes-of-Practice-2020/Health-Information-Privacy-Code-2020-website-version.pdf. Accessed on: 29 October 2021.

56. Siggins Miller. *Evaluation of the Participation Trials for the My Health Record*. Canberra: 2016. Available from: https://www1.health.gov.au/internet/main/publishing.nsf/Content/A892B3781E14E1B3CA25810C000BF7C6/$File/Evaluation-of-the-My-Health-Record-Participation-Trials-Report.pdf. Accessed on: 28 October 2021.

57. Understanding Patient Data. *Understanding Patient Data* [Online]. Available from https://understandingpatientdata.org.uk/. Accessed on: 28 October 2021.

58. British Medical Journal. Problems with care.data and other stories. *BMJ*. 2015; 351:[h4613 p.]. Available from: https://www.bmj.com/content/bmj/351/bmj.h4613.full.pdf.

59. Irish Platform for Patient Organisations, Science and Industry (IPPOSI). *Verdict from a Citizens' Jury on Access to Health Information*. 2021. Available from: https://www.ipposi.ie/wp-content/uploads/2021/09/IPPOSI_CJury_Full_Report_06092021.pdf. Accessed on: 3 November 2021.

60. The National Data Guardian. *The National Data Guardian for Health and Social*

Care Annual report 2020-2021. London: 2021. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1010375/NDG_annual_report_2020-21_v1.0_FINAL_11.08.21.pdf. Accessed on: 28 October 2021.

61. Hollo, Z., Martin, D. An equitable approach to enhancing the privacy of consumer information on My Health Record in Australia. *Health Information Management*. 2021.

62. International Association for Public Participation. *IAP2 Spectrum of Public Participation*. 2018. Available from: https://cdn.ymaws.com/www.iap2.org/resource/resmgr/pillars/Spectrum_8.5x11_Print.pdf. Accessed on: 29 October 2021.

Appendix 1 – Advisory group members

Name	Nominated Representative
Collette Tully	Royal College of Surgeons Ireland *Executive Director, National Office of Clinical Audit (NOCA)*
John Sweeney	Irish College of General Practitioners *National ICT Project Manager*
Suzanne Browne	Health Informatics Society of Ireland (HISI) Nurses and Midwives *CNIO Chief Nursing Informatics Officer*
Anne Lynott	Institute of Community Health Nursing *Director Public Health Nursing*
Colm Lawlor	Nursing and Midwifery Board of Ireland (NMBI) *Data Protection Officer*
Zetti Azvee	The College of Psychiatrists of Ireland *College of Psychiatrists Ireland (CPSYCHI) representative*
Fergus Ó'Cuanacháin	Child and Family Agency (Tusla) *Director of ICT*
Alan Reilly	Irish Pharmacy Union *Head of Information and Technology*
Derick Mitchell	Irish Platform for Patients' Organisations Science & Industry, IPPOSI *Chief Executive Officer*
Eileen O'Sullivan	Irish Platform for Patients' Organisations Science & Industry, IPPOSI *Patient Representative*
Sheila Fitzgerald	Irish Platform for Patients' Organisations Science & Industry, IPPOSI *Patient Representative*
Jacinta Hastings	National Patient Forum *Patient Representative*
Kieran Culhane	Central Statistics Office *Senior Statistician, Statistical System Coordination Unit*
Peter Connolly	Health Service Executive *Information Governance Lead*
David Hanlon	Health Service Executive

	Clinical advisor to HSE/Summary Care Record team
Yvonne Goff	Health Service Executive *Chief Clinical Information Officer of the Health Service Executive*
Roisin Doherty	Health Service Executive *Director Access to Information (A2I) and HIDs*
Noreen Noonan	Health Service Executive *ICT Programme Manager for the National EHR Programme & Lighthouse Projects*
Joe Ryan	Health Service Executive *National Director of National Services*
Niall Sinnott	Department of Health *Head of eHealth and Information Policy*
Alan Cahill	Department of Health *Senior Statistician, Statistics and Analytics Unit*
Sarah Craig	Health Research Board *Head of NHIS - National Health Information Systems*
Simon Woodworth	Health Information Systems Research Centre UCC *Director, Health Information Systems Research Centre*

Appendix 2 – Exemption examples

Exemption	Definition	Current activities, limited to the following examples:	Examples of initiatives that could be implemented with the proposed model in place:
Identification, prevention, control and surveillance of population health and disease	The use of information to support the identification, prevention, control and surveillance of population health and disease, including both communicable and non-communicable diseases.	National data collections, where there is a **statutory obligation** for data to be collected, such as the National Cancer Registry Ireland, the National Cancer Screening Programmes, Computerised Infectious Disease Reporting (CIDR), and the HSE COVID-19 Test and Trace Facility.	**Virtual disease registries and other national health databases,** whereby a nationally coordinated approach to disease surveillance is taken and the data collections are embedded into Ireland's health information systems. This would enable trends in the incidence of particular diseases and conditions that represent a high burden of disease in the general population and/or are associated with high costs for the health service (for example diabetes, cardiovascular diseases, stroke, arthritis, asthma, dementia) to be monitored over time in the most efficient and cost-effective way. With the appropriate governance and infrastructure for anonymisation, linkage and secure sharing of data, these data collections would have multiple secondary uses for the identification, prevention, control and surveillance of population health. In addition to enabling patterns and trends in the incidence of the specific diseases and conditions to be monitored over time, this initiative would lead to a greater understanding of the associated causes and risk factors, and ultimately, inform the development of evidence-based prevention and treatment strategies.

Exemption	Definition	Current activities, limited to the following examples:	Examples of initiatives that could be implemented with the proposed model in place:
Compilation or analysis of statistics relevant to health and social care	The collection, compilation, analysis or interpretation of data, expressed in either numerical or non-numerical form, relevant to health and social care.	Compilation of official statistics for which there is a **legislative framework** for the CSO to work under, including births and deaths statistics, and general health and wellbeing statistics.	**Maximising the value and increasing the scope of existing sources of statistics relevant to health and social care,** by introducing appropriate governance and infrastructure and formalised application processes to facilitate increased access for clinicians, service managers, policy makers, researchers and others involved in health service planning. This will increase the amount and type of essential statistics that are generated about health and social care in Ireland, which can be used to inform policy and enable evidence-based decision-making for the public and professionals. Examples of such statistics include: ▪ Trends in life expectancy and the impact of factors such as occupation, illness, and drug mis-use; ▪ Patterns and trends in ill-health and death by measures of socio-economic status; ▪ Childhood, infant and perinatal mortality; ▪ Long-term outcomes relating to maternal morbidity; ▪ Health and social disparities for people affected by disability; ▪ Hospital activity (admissions, emergency department presentations) ▪ Overall health and well-being.

Exemption	Definition	Current activities, limited to the following examples:	Examples of initiatives that could be implemented with the proposed model in place:
			Accurate, comprehensive, high-quality data and statistics are key to informing evidence-based public health policy, and will help achieve better social and health outcomes and reduce health inequalities.
Management and planning of health and social care services	The use of information to inform the planning, monitoring, delivery, improvement, auditing and evaluation of health services.	Assessing **eligibility** for services, for example the Primary Care Reimbursement Service (PCRS). **Service planning**, for example managing wait-lists, and the HSE Winter Plan.	**Maximising the value and increasing the scope of existing sources of health and social care information,** by introducing appropriate governance and infrastructure and formalised application processes to facilitate increased access for clinicians, service managers, policy makers, researchers and others involved in health service planning. This will increase the amount and type of essential information that is generated about the patterns of use of health and social care services in Ireland. Examples include: ▪ **Using ePrescribing data to identify inappropriate prescribing practices and adverse drug events.** For example, ePrescribing data could be analysed to identify incidences of polypharmacy in older adults and to monitor the prescribing of medications which are associated with serious adverse events in older adults. Furthermore, by linking ePrescribing data with hospital administrative datasets or summary care records / EHRs (when implemented), patients that experience adverse events

Exemption	Definition	Current activities, limited to the following examples:	Examples of initiatives that could be implemented with the proposed model in place:
			after being newly-prescribed certain types of medications in primary care could be identified. ▪ **Using administrative data to explore health service use and associated costs in certain groups.** For example, a secondary analysis of hospital administrative datasets or summary care records/electronic health records (when implemented) could identify risk factors for repeat emergency department presentations or hospital admissions among high-risk groups, such as older adults or people with specific diagnoses. Additional information could be ascertained using data linkage techniques to link population-based registries, such as the National Cancer Registry, with hospital administrative datasets or EHRs (when implemented), to accurately quantify health service use and costs associated with certain diseases and conditions.
Health and social care professional education and training	The use of information to develop resource materials, or the sharing of information during structured professional	Clinical (practice) audits; case reviews.	The new legislation should include and provide clarity around this category.

Exemption	Definition	Current activities, limited to the following examples:	Examples of initiatives that could be implemented with the proposed model in place:
	development activities, to support the education and training of health and social care professionals.		
Alternative legislative basis for the collection, use and sharing of personal information	The collection, use and sharing of personal information is required under alternative legislation.	Court order, legal proceedings, including family law cases.	The new legislation should include and provide clarity around this category.

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

For further information please contact:
Health Information and Quality Authority
George's Court
George's Lane
Smithfield
Dublin 7
D07 E98Y

+353 (0)1 8147400
info@hiqa.ie
www.hiqa.ie