Health Information and Quality Authority

An tÚdarás Um Fhaisnéis agus Cáilíocht Sláinte

Health Information and Standards

Evidence Synthesis:

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 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 in Ireland, 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

1. Introduction

A major challenge for healthcare in Ireland today is striving to achieve an appropriate balance between the protection of personal health and social care information and the use and sharing of such information to improve care. Health and social care information 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.

Advances in digital technologies have the potential to improve the quality of care provided and to also promote organisational efficiency. As health information systems are becoming more integrated and advances are made in relation to eHealth, it is important to ensure that individuals are fully informed about the collection, use and sharing of their information. Therefore, there is a need to establish, define and clearly communicate the following: the basis for the collection, use and sharing of health information; how privacy will be protected; and the benefits of sharing health and social care information. As systems evolve and practices change, ongoing engagement is necessary to monitor and evaluate the public's views and opinions in the area of health and social care information.

For the purposes 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.

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

This evidence synthesis is to inform the Health Information and Quality Authority's (HIQA's) development of recommendations on a consent model for the collection, use and sharing of health information in Ireland. These recommendations will apply to the collection, use and sharing of health information which has been processed for the purpose of providing direct care, and subsequently used for reasons beyond direct care. Legislation has already been enacted in Ireland in respect of the processing of personal

information for research purposes, in the form of the Health Research Regulations.[2] Consequently, the use of personal information for health research is not included in the scope of these recommendations. However, the use of personal information for research purposes will be discussed at stages throughout this evidence synthesis paper to provide a comprehensive picture of the use of health information beyond direct care.

1.1 Basis for collection, use and sharing of health information

The collection, use and sharing of personal health information is essential for high-quality health and social care services. In order to provide safe and effective care to the individual, health and social care professionals need relevant information available to them when making decisions. Consequently, people need to provide health and social care professionals with confidential personal information. This personal health information is collected and recorded in paper-based and or electronic records. When clinical or care decisions are required, the health information is used by and shared between professionals providing and managing care. Individuals expect health and social care professionals and organisations to communicate effectively with each other to provide a high standard of care. The use of health information in this respect is to provide **direct care**[*].

Sharing of health information for **uses beyond direct care**[†] is also very important for the effective functioning and management of the health and social care system, as it helps to promote the safe and effective provision of care. This means that the information collected for individual care is shared and used for other purposes. Some examples include for health and social care planning and management, the evaluation and improvement of services, policy development and research.

1.2 Benefits of sharing health information

For direct care purposes, it is in an individual's best interests that personal information is collected, used and shared appropriately. When professionals do not have access to the most relevant and up-to-date information, it can result in duplication of efforts and suboptimal delivery of care. For example, tests and scans may be repeated which can delay care and treatment, as well as increasing costs and negatively impacting on the efficiency of services.[3] It can also be inconvenient for individuals as they have to continuously relay their care history during consultations. Sharing personal information in a secure and controlled manner is an integral part of effective care provision.

Using health information for reasons beyond direct care in a safe and controlled manner has many benefits, including health and social care services operate effectively and efficiently; people receive high-quality and safe care; and the most appropriate and effective treatments are available. For example, information is used by management within the Health Service Executive (HSE) to review waiting lists and organise resources,

[*] This is referred to as the primary use of health information in some jurisdictions.
[†] This is referred to as the secondary use of health information in some jurisdictions.

such as operating theatres, to ensure they are used to optimum 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 the best level of care, such as the development and implementation of national clinical guidelines.[4]

1.3 Protecting privacy

Although the collection, use and sharing of personal health information is essential, there is a need for strict rules and procedures to ensure these processes occur in a safe and controlled manner. Health and social care provision depends on trust. People should be assured that they can discuss sensitive matters with their health and social care professionals without fear of this information being inappropriately used and shared. 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.

Data protection is a fundamental right set out in Article 8 of the European Union (EU) Charter of Fundamental Rights.[5] Under the General Data Protection Regulation (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.[6] 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 share and use 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.

Professionals, however, need to share personal health information with other professionals or teams supporting the provision of care. There should be clear rules to protect privacy, outlining when and how information can be shared, and these should be detailed through a comprehensive framework including legislation, codes of practice, policies and procedures. There also needs to be adequate security in place to protect

against known and potential risks of both paper-based and electronic health records (EHRs). As professionals are bound by confidentiality agreements, they should only use and share personal health information if they have the authority and a reason to do so.

The use and sharing of health information for purposes beyond direct care does not always require personal information. For certain uses beyond direct care, in order to protect an individual's privacy, health information can be changed to make it difficult or impossible to identify the individual about whom it was collected. Health information can be pseudonymised, anonymised and de-identified (see glossary of terms for definitions). This means that identifiable information can be removed before sharing this information or other techniques can be used to prevent re-identification. The information can then be used and shared in a secure manner, ensuring privacy is protected. When personal information is required for purposes beyond direct care, such as the planning and management of health and social care services, it must be shared in line with data protection legislation and regulations.

In some situations, it is important to ask the individual if they agree for their personal information to be used and shared. In the GDPR, this process is referred to as seeking consent for processing of data and is defined as: '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'.[7] It is important to note also that, under GDPR, if health information can be 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 or other de-identifying techniques can be used to prevent re-identification.[8] This means that, with the correct data governance, the data can then be used in a safe and secure manner, ensuring privacy is protected[‡].[9]

Consent is typically 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 through individual actions. 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.

The principles of data protection, such as transparency and confidentiality, are important regardless of which consent approach is applied.

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

The process of seeking consent for health information is evolving in jurisdictions, particularly in jurisdictions where eHealth models have progressed. It can involve a once-off or fixed arrangement or it can be a dynamic process. 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.[10] In relation to health information, this model involves ongoing engagement and communication between individuals and the users and custodians of their information. This can operate in a safe and controlled manner applying exemptions when the information is required; for example, in an emergency or for public health reasons. Dynamic consent has been explored primarily within medical research, in fields such as bio-banking and genomics, where ongoing contact is required with participants.[10] However, it is now also being used in the area of health information as people are increasingly being provided with opportunities to actively manage the use and sharing of their personal health information through online portals.[11]

Opt-out consent 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.[12] It is important to note, however, that there is currently significant international debate about the appropriateness of opt-out consent models, both in relation to EHRs and the use of health information beyond direct care. Among proponents of an opt-in consent approach to initiation of EHRs, arguments against an opt-out consent approach centre on the security of health data in centralised record systems.[13,14] In some jurisdictions, there has been a move away from opt-in approaches due to poor uptake; without high levels of uptake of EHRs, there is a risk that the significant advantages that an EHR can offer will not be realised.[15] In addition, both opt-in and opt-out consent approaches for EHRs may be associated with a patient safety risk. If a person refuses to opt in, or chooses to opt-out, of having one, their clinical 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.[16]

In relation to an opt-out consent model for the use of information beyond direct care, 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.[17] A further disadvantage of this approach is that 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.[12] As such, it is important that countries take into account multiple factors and perspectives when deciding on what consent approach to take when implementing eHealth initiatives

and changes to information sharing. Appropriate engagement is necessary to address potential barriers and maintain people's rights to privacy.[17]

1.4 Public engagement

The collection, use and sharing of health information is a complex and dynamic area. Advances in technology bring about new capabilities in relation to the use of information for both direct care and beyond direct care. People's perceptions, experiences and opinions in relation to health information are constantly evolving as new advances are made. As previously stated, the model for the collection, use and sharing of health information should follow a rights-based approach. It is vital that the public are involved in any decisions in this area to ensure they are underpinned by people's rights in relation to personal information and are viewed as acceptable and trustworthy by the public.

International evidence highlights that public engagement in relation to the collection, use and sharing of health information is an extremely important element of building a culture of trust when developing a consent model.[9] Public engagement helps to understand what level of trust currently exists and what is acceptable to people in relation to their health information.[12] It also plays an important role in educating the public on the benefits of information sharing across the health system so that there is a universal understanding. Such an approach can inform the implementation of new technologies and initiatives, such as EHRs and a citizen health portal, as challenges and opportunities can be identified and addressed. Countries that have implemented successful health information initiatives have undertaken significant and ongoing engagement with the public.[17,18]

Public engagement describes a spectrum of approaches in which people are involved in informing decision-making. Figure 1 outlines a framework, developed by the International Association for Public Participation (IAP2),[19] that details different approaches to public engagement. 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. Successful engagement processes appear to move beyond solely informing the public towards approaches that involve, collaborate and empower individuals. Engagement must be ongoing in order to build and maintain public trust and respond to people's needs.

Figure 1: IAP2 Spectrum of Public Participation[19]

	Inform	**Consult**	**Involve**	**Collaborate**	**Empower**
Public Participation Goal	To provide the public with balanced and objective information to assist them in understanding the problem, alternatives, opportunities and/or solutions.	To obtain public feedback on analysis, alternatives and/or decisions.	To work directly with the public throughout the process to ensure that public concerns and aspirations are consistently understood and considered.	To partner with the public in each aspect of the decision including the development of alternatives and the identification of the preferred solution.	To place final decision-making in the hands of the public.
Promise to the Public	We will keep you informed.	We will keep you informed, listen to and acknowledge concerns and aspirations, and provide feedback on how public input influenced the decision.	We will work with you to ensure that your concerns and aspirations are directly reflected in the alternatives developed and provide feedback on how public input influenced the decision.	We will look to you for advice and innovation in formulating solutions and incorporate your advice and recommendation into the decisions to the maximum extent possible.	We will implement what you decide.

Increasing impact on the decision

2. Methods

2.1 Aim

The purpose of this document is to outline the evidence from research performed throughout the process of developing the recommendations on a consent model for the collection, use and sharing of health information in Ireland.

2.2 Evidence review

There were three aspects to the evidence synthesis, which are outlined below.

Firstly, an international review was undertaken to identify how a number of jurisdictions define key terms associated with the development of a model for health information in their legislation. The key terms chosen for this review were: 'health information', 'use of information for direct care' and 'use of information beyond direct care'. Section 3 discusses the different definitions used in the eight jurisdictions included in the international review (outlined below) and identifies the concepts that are considered important when defining each of these terms.

Secondly, an 'as-is' analysis was carried out to understand the current situation in place in Ireland regarding the collection, use and sharing of health information. The 'as-is' analysis is presented in Section 4.

Thirdly, an international review of consent models for the collection, use and sharing of health information was performed and published in 2020 to identify examples of best practice, which can be found on www.hiqa.ie here. The jurisdictions included in the review were:

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

An update of the international review was completed in 2021, where a desktop review was performed to identify any changes or planned changes to practices in each jurisdiction. Experts were contacted in each jurisdiction to validate the evidence prior to publication. Section 5 presents a summary of international evidence by theme: legislation; governance structures; eHealth initiatives; consent models; and public engagement.

3. Review of international definitions

This section describes approaches to defining key terms for health information in other jurisdictions and identifies the concepts that are important when defining each term. The key terms chosen for this review were: 'health and social care information', 'use of information for direct care' and 'use of information beyond direct care'.

3.1 Health and social care information

The definition of health and social care information differs across the eight jurisdictions included in the international review. The definition, or description, used by each jurisdiction included in the review is presented in Appendix 1. All jurisdictions 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".[20] 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.[21] In Australia, an individual's expressed wishes about the future provision of healthcare is also incorporated into the definition.[22,23] Some jurisdictions specifically include a reference to how information is recorded. For example, England and Northern Ireland include 'information (however recorded)' in their legislation.[24-26] This may be an important element to help future-proof legislation alongside the introduction of different methods of recording information, such as electronic records.

The key concepts included in current definitions across jurisdictions 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. Some jurisdictions have included information specific to their healthcare context. For example, in Ontario (Canada), payments or eligibility for healthcare or coverage for healthcare is cited in their legislation,[27] and genetic information is included in the Australian definition.[22,23]

3.2 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. The definition, or description, used by each jurisdiction is presented in Appendix 2. There are differences, however, across jurisdictions on what activities are included within direct care. In some jurisdictions, activities that inform the wider provision of care are considered sufficiently connected to the provision of direct care as long as they are conducted by someone with a 'legitimate care relationship' to the individual. 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. 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.[28] 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 an essential element of direct care in many jurisdictions.

3.3 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 define this use of health information in legislation and they refer to it as 'the secondary use' of health information.[28,29] All jurisdictions outline the permitted uses of health information beyond direct care in legislation although the depth of detail differs between jurisdictions. For example, Estonia and Northern Ireland provide examples of the types of uses that are permitted without specifying exact activities.[20,28,30] In all other jurisdictions, a specific list of the permitted uses beyond direct care is outlined in legislation. The definition from each jurisdiction is presented in Appendix 3.

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 appear to be the most common uses of health information beyond direct care. A number of additional uses were also identified that are unique to particular jurisdictions. For example, development and innovation activities are considered a secondary use in Finland where engineering and business data can be combined with existing data, including personal data, for the purpose of developing products, processes, or services.[29] Processing payment claims for healthcare is cited as a secondary purpose in Ontario (Canada).[27]

3.4 Summary - Review of international definitions

The definitions of health information, and definitions of the uses of information for direct care and beyond direct care, were seen to differ between jurisdictions. Differences in the definitions likely reflect the need to develop definitions that are relevant to the health and social care system in which they apply. It is possible, however, to identify some common concepts across jurisdictions for each of these terms, which likely represent those elements of key importance. It is important that there is a consistent understanding of these terms in the development of a model for the collection, use and sharing of health information to support the appropriate and effective use of information.

4. As-is analysis – collection, use and sharing of health information in Ireland

4.1 Legislation

Table 1 outlines relevant legislation in relation to health and social care information in Ireland. The collection, use and sharing of health information for the purposes of direct care and beyond direct care have been addressed in different legislation across both general information and health legislation with limited health information-specific legislation in place.

Table 1. Summary of relevant legislation in relation to health information in Ireland

General information legislation	Health legislation (including aspects relating to health information)	Health information legislation
▪ Data Protection Acts, 1988 - 2018 ▪ Statistics Act 1993 ▪ Civil Registration Act 2004 ▪ General Data Protection Regulation (GDPR) 2018 ▪ European Union (Measures for a High Common Level of Security of Network and Information Systems) Regulations 2018 ▪ Data Sharing and Governance Act 2019 ▪ European Union (Open Data and Re-use of Public Sector Information) Regulations 2021	▪ Health Acts 1947, 1953, 2007 ▪ Health (Duties of Officers) Order 1949 ▪ Infectious Disease Regulations 1981 ▪ Medicinal Products (Prescription and Control of Supply) Regulations 2003 (as amended) ▪ Misuse of Drugs Regulations 2017 (as amended) ▪ Patient Safety (Notifiable Safety Incidents) Bill 2019	▪ Health (Provision of Information) Act 1997 ▪ Health Identifiers Act, 2014 ▪ Health Research Regulations 2018

4.1.1 General information legislation

The Data Protection Act 2018,[31] incorporating the GDPR,[7] governs the collection and processing of personal information. This legislation details the specific standards of data protection for individuals and obligations of organisations that process personal data.

The Act also established the Data Protection Commission as the data protection authority responsible for supervision and enforcement of the data protection standards.

GDPR sets out seven general principles which must underpin the collection, use and sharing of personal information:

- **Lawfulness, fairness, and transparency**: there must be a legal basis for the collection, use and sharing of information and it should be used in a fair and transparent manner.
- **Purpose limitation:** information must only be collected for specific purposes, and should not be further used and shared unless it is compatible with the original purpose and in line with individuals' reasonable expectations.
- **Data minimisation**: the collection, use and sharing of information should be limited to only what is necessary for the purposes for which it is required.
- **Accuracy:** information must be accurate and steps must be taken to ensure any inaccuracies are dealt with promptly and appropriately.
- **Storage limitation:** information should only be stored for the minimum time necessary.
- **Integrity and confidentiality**: appropriate measures should be in place to ensure the integrity and confidentiality of information.
- **Accountability**: ensures compliance with data protection principles and appropriate processes and records are in place to demonstrate accountability.

Under the GDPR, health data is considered a special category of personal data and there are specific conditions attached to its processing.(7) 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 if one of the following applies:

- the data subject has given explicit consent to the processing of those personal data for one or more specified purposes
- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller
- processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent
- processing is necessary for reasons of substantial public interest
- processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis,

the provision of health or social care or treatment or the management of health or social care systems and services on the basis of European Union or Member State law or pursuant to contract with a health professional

- processing is necessary for reasons of public interest in the area of public health
- processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

The Data Protection Act 2018 provides more specific details on the use and sharing of personal health information in Ireland.[31] Once key data protection principles are maintained, as outlined above, personal health information may be used and shared for the following purposes, if undertaken by a healthcare professional or someone that is bound by the same duty of confidentiality as a healthcare professional:

- preventative or occupational medicine
- assessment of the working capacity of an employee
- medical diagnosis
- provision of medical care, treatment or social care
- management of health or social care systems and services
- if related to a contract with a health practitioner.

The Statistics Act 1993 officially established the Central Statistics Office (CSO).[32] Under the Act, the CSO is permitted to collect personal health information, such as births and deaths of individuals, information on disability, carers and voluntary activities, and information on health and social conditions, for particular uses such as generating statistics on acute hospital services.

The Civil Registration Act 2004 formally established the Civil Registration Service and introduced an improved system to maintain, manage and control civil registration, including births, stillbirths, adoptions, marriages, decrees of divorce or nullity and deaths.[33] This legislation outlines the specific information that should be collected during the registration process and allows for the compilation and publication of statistics in relation to this information; these are termed 'vital statistics'. Identifiable information from the registration system may be shared for the purposes of medical or social research or to medical officers of health boards if permission is provided by the Minister for Health.

The European Union (Measures for a High Common Level of Security of Network and Information Systems) Regulations 2018 outline the security measures that operators of essential services, such as healthcare providers, are required to meet to ensure a common high level security of network and information systems across European

Member States.[34]

The Data Sharing and Governance Act 2019 provides a legal basis for the sharing of administrative data between public bodies, including the HSE and government, where the sharing is for the performance of a function of either of the public bodies.[35] The Act allows the sharing of personal data under certain circumstances, such as verification of identity, establishing individual entitlement to a public service, facilitating the administration, supervision and control of a service, programme or policy, and facilitating the improvement or targeting of a service, programme or policy. This Act only applies to the special categories of data outlined in the GDPR, such as health data, in particular circumstances, such as establishing a personal data access portal and enabling individual access to same, and prescribing rules, procedures and standards in relation to base registries, the conduct of data protection impact assessments by public bodies and the processing of personal data by a public body.[7] Any sharing of information must be undertaken in accordance with a data-sharing agreement entered into by the public bodies concerned and the Act provides a comprehensive outline of what should be included in a data-sharing agreement. The Act provides for the establishment of the Data Governance Board which will review these data sharing agreements.

The European Union (Open Data and Re-use of Public Sector Information) Regulations 2021 address a number of barriers to the re-use of publicly-funded information and bring the legislative framework in line with advances in digital technologies.[36] Under these regulations, the re-use of information held by public bodies, including publicly-funded research data, should be free of charge. In addition, there is now an obligation on public sector bodies to make public data available as open data, and as 'dynamic', meaning that the data should be updated frequently and in real time. It does not apply to personal data, as defined by GDPR.[7]

4.1.2 Health legislation

Under the Irish Health Acts 1947 and 1953,[37,38] the Health (Duties of Officers) Order 1949,[39] and the Infectious Disease Regulations 1981,[40] the Medical Officer of Health has the responsibility to investigate and control notifiable infectious diseases. Under the Infectious Disease Regulations 1981, all medical practitioners, including clinical directors of diagnostic laboratories, are required to notify the Medical Officer of Health and or Director of Public Health of certain diseases.[40] The list of diseases (and their respective causative pathogens) that are notifiable is contained in the Infectious Diseases Regulations 1981 and subsequent amendments. Notification requires sharing of personal information and relevant clinical information. Information is subsequently shared with the Health Protection Surveillance Centre (HPSC) and may be shared with health authorities outside of Ireland. In general, identifiable information is not shared in these circumstances and is only shared if required for contact tracing.

Under the Health Act 2007 (as amended),[1] HIQA may request health information from the HSE or a healthcare provider in line with its functions outlined in the Act.

HIQA's functions include: setting standards for health and social care services; regulating and monitoring health and social care services; completing health technology assessments; and advising on the efficient and secure collection and sharing of health information.

More recently, as a response to restrictions imposed due to COVID-19, temporary amendments were made to regulations for the Medicinal Products (Prescription and Control of Supply) Regulations 2003 (as amended) and the Misuse of Drugs Regulations 2017 (as amended) which allowed for the sharing of prescription information between General Practitioner (GP) practices and pharmacies via email.[41,42]

4.1.3 Health information legislation

The Health (Provision of Information) Act 1997 allows for the provision of information to the National Cancer Registry Ireland (NCRI) without the consent of the service users concerned as cancer prevention is considered an overriding public interest.[43] This Act allows the National Cancer Registry Board, the Minister for Health, a health board, hospital or other body or agency participating in any cancer screening programme authorised by the Minister for Health to request information from data controllers or data processors in order to fulfil their functions in relation to cancer screening.

The Health Identifiers Act 2014 provides for the assignment of unique health service identifiers to individuals to whom a health service is being, has been or may be provided and for the assignment of unique identifiers to health services providers.[44] The individual health identifier (IHI) is primarily used for the provision of direct care. If the IHI is required for use beyond direct care, a separate application must be made to the Department of Health. This Act permits health service providers and other entities, including the Health Research Board (HRB) and the NCRI, to provide an individual's health service identifier or other identifying particulars to an authorised disclosee in order to enable the processing of such information for use beyond direct care. Authorised disclosees include the CSO and health profession regulatory bodies.

The introduction of the EU Cross-Border Directive 2011/24/EU in 2011 on the application of patients' rights in cross-border healthcare allows for EU citizens to access healthcare in EU states other than those in which they are normally resident.[45] It promotes the sharing of health data between different care providers and member states and forms the basis for the establishment of the European National Contact Point Programme. The Irish Open National Contact Point (open NCP) infrastructure has been established and Ireland has committed to develop the infrastructure to enable transmitting health data to another member state, such as summary care records and electronic prescribing data.

The Data Protection Act 2018 provides for the Health Research Regulations 2018 which outline the suitable and specific measures for the processing of data for health research.[2] The processing of personal data for health research purposes requires that consent must be adequately informed and appropriately recorded; therefore explicit

consent must be obtained from the individual whose data are to be processed. The regulations also provide for circumstances where the research is considered to be of significant public interest but obtaining explicit consent is not feasible. In those instances, applications can be made to the Health Research Consent Declaration Committee (HRCDC) which makes a decision on whether explicit consent is required. The Department of Health also intends to develop two further sets of regulations on the use of health information for individual care and for service planning which would aid a greater use of health information and support integrated care in a secure and confidential manner.

Plans for a Health Information and Patient Safety Bill have been in existence since 2007 and subsequently evolved to become the Health Information and Patient Safety (HIPS) Bill.[46] The HIPS Bill had a range of measures relevant to health information including the provision of a regulatory framework for 'data matching', which is described as personal information gathered for one purpose by a health organisation that is later 'matched' with personal information gathered for a different purpose by the same organisation. In 2017, the HIPS Bill underwent a public consultation where concerns were raised regarding the buying and selling of personal health data, compliance with GDPR and the lack of mechanism for establishing 'a prescribed data matching programme' or a prescribed health information resource. Consequently, the HIPS Bill was not enacted in its original form.

It was changed and informed the development of the Patient Safety (Notifiable Safety Incidents) Bill 2019.[47] This Bill will mandate the open disclosure of certain adverse safety incidents occurring in the course of the provision of a health service to a person, in both the public and private sector. It contains an exemption to the Freedom of Information legislation for a record that is a clinical audit (where patient care and outcomes are compared against explicit standards). The Bill is currently before Dáil Éireann, the Government of Ireland.

4.2 Governance structures

4.2.1 General information

There are specific data governance structures in Ireland which have a broad remit and cover all sectors.

The Data Protection Commission is responsible for supervision and enforcement of the data protection standards. The Data Sharing and Governance Act 2019 provides for the establishment of a Data Governance Board who will review data sharing agreements for the sharing of administrative data between public bodies. This Board can appoint sub-committees and there are plans in place to establish a data sharing sub-committee who will review data sharing agreements for legal compliance and report to the Board.

In addition, an Open Data Governance Board (ODGB) has been established to provide strategic leadership and governance in line with best international practice in the area of Open Data, and oversees the implementation of the national Open Data Strategy. In

2022, the ODGB will renew the national Open Data Strategy to take account of the obligations for public sector bodies in the EU (Open Data and Re-use of Public Sector Information) Regulations 2021. As part of the new Open Data Strategy, forums and communities of data processors and re-users will be established.

4.2.2 Health information

Currently, there are multiple agencies with responsibility for health information in Ireland. The Department of Health is responsible for health information policy. The HSE is responsible for implementing national health information systems across the entire health and social care system. HIQA has a remit under the Health Act 2007 to develop recommendations, standards and guidance on health information, and assess compliance with those national standards.

The eHealth Strategy, published in 2013, originally called for a single entity (eHealth Ireland) to be established, outside of the HSE, with a legislative remit to provide strategic leadership and governance to support the collection, use and sharing of health information in Ireland.[48] To date, eHealth Ireland has not been formally established as a separate entity to the HSE. HIQA's position paper 'The need to reform Ireland's national health information system to support the delivery of health and social care services' once again highlights the significant need for robust strategic leadership and governance for health information.[3] The position paper recommended 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 strategic leadership and governance for health information, HIQA states that 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.

In relation to the governance of health information, the principles of data protection which are set out in GDPR and the Data Protection Act 2018 must be adhered to. In terms of accountability for the management of information, GDPR sets out the requirements for the designation of a Data Protection Officer (DPO) for any organisation that processes personal data. In terms of an established network for data governance for services, there is a DPO and four Deputy DPOs in the HSE.

Within the HSE, the overall accountability for the collection, use and sharing of health information lies with Senior and Local Accountable Officers in line with the Delegation and Performance and Accountability Frameworks.[49,50] Accountable Officers are fully responsible and accountable for the services they lead and deliver. Hospital Group Chief

Executive Officers (CEOs) are considered Senior Accountable Officers and responsible for their hospital group. Community health organisation (CHO) Chief Officers and the heads of national services, including National Ambulance Service, Primary Care Reimbursement Service (PCRS), Environmental Health, Public Health, Nursing Home Support Service and the National Screening Service, are considered the Senior Accountable Officers for their areas of responsibility. Local Accountable Officers are accountable at a hospital or local service level. In addition, information governance committees are in place in many health and social care services; however, these structures vary across local services. Nationally, the HSE Performance and Delivery Committee has a role in monitoring the implementation of the Performance and Accountability Framework with a focus on improved governance.

In relation to the use of information beyond direct care, the Department of Health and CSO convene a Health Data Liaison Group which comprises members from various stakeholder organisations across Ireland and is responsible for assessing the needs of key users of health information and developing the statistical potential of information sources in this field. This liaison group has no responsibility in relation to the governance of the use of information beyond direct care.

In line with the Health Research Regulations 2018, a committee was established to govern the processing of personal health information for research purposes. The HRCDC reviews applications from researchers who wish to obtain a consent declaration, which means that explicit consent is not required for the obtaining and use of their personal information for the health research concerned. All applicants must demonstrate to the HRCDC that the public interest of doing the research outweighs the need for consent.

In addition, a recent partnership between the HRB, the CSO and the Department of Health has led to the establishment of a Research Data Governance Board (RDGB) to coordinate and facilitate secure and controlled access to data contained within a COVID-19 Data Research Hub, which is maintained by the CSO.

A scoping report conducted by the HSE on research governance highlighted that there is no relevant research governance framework for all HSE and associated organisations.[51] The authors state that this has led to a lack of clarity in relation to roles and responsibilities and the absence of a standardised and reliable approach to research governance. It recommended the development of a data governance policy for the health service, and appropriate procedures and structures in place at local, regional and national levels to support robust governance arrangements.

4.3 eHealth initiatives in Ireland

In Ireland, there is currently a mix of paper-based and electronic healthcare records in place. There are plans to invest further in eHealth with the recent Sláintecare Implementation Strategy and Action Plan 2021-2023 outlining a number of eHealth and technology actions that will be progressed. Table 2 outlines the different eHealth initiatives that are in place, or planned, in Ireland.

Table 2. Summary of eHealth Initiatives in Ireland

National health identifier	Electronic Health Records	ePrescribing	eReferral	Examples of planned eHealth initiatives [52]
✓ Individual Health Identifier – **partially implemented**	✓ Maternal and Newborn Clinical Management System - **partially implemented**	✓ ePrescribing – **partially implemented**	✓ National Electronic Referral Programme	▪ Summary and Shared Care Records (SCRs) ▪ Citizen Health Portal ▪ Electronic Discharge System

Descriptions of some of the key eHealth initiatives are outlined in the following sub-sections with an overview of their current status, where relevant.

4.3.1 Individual health identifiers

The Health Identifiers Act was passed in 2014 which legislated for the creation of individual health identifiers (IHIs), which are unique personal numbers used across all public health and social services.[44] The Health Identifier Office was set up in 2019. The technical infrastructure for the Health Identifier Index is in place and is populated with 6.7 million IHIs relating to current and former residents of Ireland. Use of the IHIs has only been partially implemented to date but their continued rollout as part of the eVaccination Programme has been given initial priority in the Sláintecare Strategic Action Plan 2021–2023.[52]

4.3.2 Electronic Health Records (EHRs)

Currently, the only established EHR in place in Ireland is the Maternal and Newborn Clinical Management System, an EHR for all women and babies being cared for in maternity services in Ireland. It was first implemented in 2016 and is currently being rolled out across all maternity services in Ireland. The implementation of the national acute EHR was initially prioritised as part of the Sláintecare Implementation Strategy, starting with the new National Children's Hospital, and community-based EHRs to support integration, care in the community and to support better acute demand management.[53] Prioritisation on the EHR programme has changed with the focus now on delivering the summary and shared care record programmes in the new Sláintecare Implementation Strategy and Action Plan 2021–2023.[52]

4.3.3 National Electronic Referral Programme

The National Electronic Referral (eReferral) Programme is a national programme that allows all acute hospitals to accept referrals electronically.[54] It was first piloted in 2011 and has continued to grow. GPs across the country can now refer patients into every acute hospital electronically using an approved referral form and immediately receive an acknowledgement confirming receipt of same. Specialist eReferral forms have been developed for specific procedures, such as endoscopy, which provide the receiving clinician with more speciality-specific information in order to improve the patient triage process. The eReferral programme is underpinned by Healthlink, which is a web-based messaging service which enables the secure transmission of clinical information. Healthlink also includes a Lab Order functionality which allows GPs and practice nurses to order blood tests online rather than using a manual order form. The use of Healthlink for these functions ensures referrals and order forms are legible and complete which helps to achieve safe and timely care.

4.3.4 Electronic prescribing

Electronic prescribing (ePrescribing), the process of sending medical prescriptions from healthcare professionals, was identified as a national eHealth priority as part of the eHealth Strategy,[48] and an ePharmacy programme was established within the Health Service Executive in 2015. However, ePrescribing in community pharmacy is still not implemented in Ireland. Due to COVID-19 related restrictions, there was an urgent need for electronic prescribing and temporary amendments were signed into law (regulations) to allow for the transmission of digital prescriptions, namely the Medicinal Products (Prescription and Control of Supply) Regulations 2003 (as amended) and the Misuse of Drugs Regulations 2017 (as amended).[41,42] However, such actions only offer a temporary solution. There exists a legal requirement in Ireland to produce a paper prescription for people to present to their pharmacist. Legislation is currently being drafted to allow for ePrescribing and a review of the existing temporary process is needed to inform such legislation and subsequent implementation. ePharmacy and ePrescribing have also been identified as key eHealth actions in the Sláintecare Implementation Strategy and Action Plan 2021–2023.[52]

4.3.5 National health email service

A national health email service, known as Healthmail, has been implemented which is a secure email service that allows healthcare providers to send and receive identifiable clinical information. It was initially developed for GPs and their support staff but it is now available to community pharmacies, nursing homes and optometrists. It plays a key role in reducing the need for outpatient referrals by providing a secure medium for clinical communication between GPs and secondary care. COVID-19 emergency legislative provisions recognised Healthmail as a national electronic prescription transfer service, and was used to support the COVID-19 response by providing a secure mechanism for sharing demographic data within the HSE itself and with external organisations, such as long-stay residential facilities. This has been used extensively to support COVID-19

testing for the residents and staff of long-stay residential facilities, such as nursing homes and the sharing of contact data for contact tracing purposes. Further, there is infrastructure in place to support European cross-border exchange of health information.

4.3.6 Future opportunities

While all of the initiatives outlined above are positive developments in the eHealth landscape, there are a number of key areas where greater progress is needed. Ireland is only at the stage of developing a policy for a national EHR and is one of just three countries in the European Union without a national system that provides service users with access to their EHRs, such as a digital portal.[55] In its strategic priorities, the National Statistics Board identified the need for a comprehensive national infrastructure for health and related data.[56] It noted that the lack of a comprehensive infrastructure for secure data access, storage, sharing and linkage of routinely collected health, social care and related data is a challenge for health research leading to delayed and incomplete policy-relevant studies, as well as significant challenges for clinical care. The Central Statistics Office 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.

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 as having fragmented practices, strategies that are not fully implemented, and limited vision in using data infrastructure.[57] Results of a survey carried out by the Organisation for Economic Co-operation and Development (OECD) highlighted the fact that Ireland is lacking a central body to process and make data available in an efficient manner.[58] 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. 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, but Ireland was one of four countries that did not have this capability.[58]

There are plans in place to address some of these gaps with a robust eHealth programme seen as an essential foundation to achieving an integrated healthcare system. The Sláintecare Implementation Strategy and Action Plan 2021-2023 lists a number of eHealth and technology actions that will be progressed to support integration and provide safe and timely access to care.[52] Such initiatives include summary and shared care records, a citizen health portal, an electronic discharge system, a GP research hub, a health performance and visualisation platform and management systems for residential care and home support. Immediate priority is focused on the continued

rollout of IHIs as part of the eVaccination Programme and their subsequent use in other areas to enable the creation of shared care records.

Additionally, a proof of concept project is currently being undertaken to assess the Data Access Storage Sharing and Linkage (DASSL) model.[59] The DASSL model attempts to address the need for a safe and trusted modern infrastructure that allows use of currently underexploited health data for 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.[60] The proof of concept 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 safe havens 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 current DASSL model focuses primarily on the use of data for health research, but there are potential opportunities to broaden the scope of the model to incorporate additional uses of information beyond direct care. Learnings from the project will be important to assess the requirements for a national model to support the use of information beyond direct care.

4.4 Consent model

4.4.1 Use of information for direct care

Under the Data Protection Act 2018, personal health information can be collected, used and shared for the provision of direct care when it is undertaken by a healthcare professional or an individual who has a duty of confidentiality equivalent to a healthcare professional. Confidentiality is a key principle included in professional codes of conducts for different healthcare professionals, such as the most recent *'Guide to Professional Conduct and Ethics for Registered Medical Professionals'*.[61] Breaching confidentiality may be considered professional misconduct and can result in fitness to practice cases which are covered under relevant legislation for health and social care professionals, such as the Medical Practitioners Act 2007. Additionally, the common law duty of confidentiality applies where personal information that was given in confidence to a health or social care professional should not be shared without consent or justification. Under the common law duty of confidentiality, there is no distinction between information that is held electronically or in hard copy.

The sharing of personal health information between healthcare providers to inform care is viewed as an essential use by the Medical Council and the Irish College of General Practitioners (ICGP).[61,62] The ICGP states that "the transmission of personal data concerning health is part of the referral process and part of the practice of medicine", and, consequently, that such sharing of information does not require explicit consent.[62] While the Medical Council agrees that sharing of health information is a part of providing care, it does state that an explanation should be given to patients that information will

be shared and with whom, and that referrals or additional care might not be possible without information sharing.[61]

4.4.2 Use of information beyond direct care

Explicit consent must be obtained for the processing of personal health information beyond direct care unless one of the exemptions in the Data Protection Act,[31] GDPR,[7] or other relevant legislation applies, as detailed in section 4.1. For example, exemptions may allow the processing of personal health information without the consent of the individual for reasons of public interest in the area of public health, or for the management of health or social care systems and services. The Health (Provision of Information) Act 1997 allows the National Cancer Registry Board, the Minister for Health, a health board, hospital or other body or agency participating in any cancer screening programme authorised by the Minister for Health to request information in order to fulfil their functions in relation to cancer screening.[43] Under the Infectious Disease Regulations 1981, information on notifiable infectious diseases must be shared with the Medical Officer of Health for control and monitoring purposes.[40] Additionally, HIQA may request health information from the HSE or a healthcare provider in order to fulfil their functions laid out the Health Act 2007 (as amended).[1] Explicit consent is not required in such circumstances.

Data that has been appropriately anonymised is not considered personal data under GDPR.[7] Consequently, anonymised health data is not subject to the restrictions outlined in GDPR, and explicit consent is not required for the use and sharing of this data. The legislation, either GDPR or the Data Protection Act, does not prescribe any particular technique for anonymisation but the Data Protection Commission has developed a guidance note outlining appropriate measures to ensure data is sufficiently anonymised so as not to be considered personal data.[8]

The Medical Council views clinical audit, quality assurance, education and training as essential to providing safe and effective care.[61] It states that anonymised or pseudonymised information should be shared where possible and consent is not required in these circumstances. Where this is not possible, the patient should be informed of the disclosure and given the opportunity to opt-out. Typically, GDPR (articles six and nine) is drawn upon to inform practice in relation to consent and information sharing.

Under the Health Identifiers Act 2014, specific organisations can access the IHI for purposes beyond direct care without gaining explicit consent.[40] These organisations include the CSO, National Treatment Purchase Fund Board and the Inspector of Mental Health Services. Relevant 'secondary purposes' are listed in the Act and include promotion of patient safety, including clinical auditing and investigating and reporting patient safety incidents; management of health services; identification or prevention of a public health threat; provision of a health-related insurance scheme and processing of relevant information to protect the health or safety of an individual. Named organisations only have access to non-identifiable information. There is, however, limited use of the

IHI information beyond direct care currently as the system has only been partially implemented. Due to COVID-19, development and use of the IHI has focused on supporting contact tracing and tracking individuals along the COVID care pathway through linkage with a COVID-Identifier. Such changes have led to delays in the development of infrastructure necessary for wider sharing of information, although they allow insight into the future process of implementation.

With regard to processing of health information for research purposes, the Health Research Regulations 2018 set out specific safeguards (as required under GDPR) which must be in place before personal information can be processed for health research, including requirements for explicit consent and prior approval by a research ethics committee.[2] Where the requirement to obtain consent cannot be met, data controllers may apply to the HRCDC for a declaration that explicit consent is not needed as the public interest in carrying out the research significantly outweighs the need for consent.

4.5 Public engagement

A systematic review on public views on the use of patient data in Ireland and the UK found that there is a general willingness to share EHR data for 'secondary purposes like research, policy and planning' as it is associated with 'the greater good', although individuals want to feel in control of how their information is used.[63] The Irish Platform for Patient Organisations, Science & Industry (IPPOSI) facilitated a Citizens' Jury on Access to Health Information.[64] Jurors concluded that people must be involved in the development of relevant policies and emphasised that they should be able to actively manage and consent to the use of their information on an ongoing basis.[65]

One of the core principles set out in the Sláintecare Implementation Strategy and Action Plan 2021-2023 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.[52] HIQA, in conjunction with the Department of Health and the HSE, carried out the first National Public Engagement on Health Information in Ireland in 2020 and 2021.[66] The findings are available on www.hiqa.ie. The findings show that the vast majority of people in Ireland are happy for their health information to be used and shared for their direct care and for certain purposes beyond their direct care. However, most people want to be informed about how their information will be used and shared and that there are systems in place to protect the privacy and security of their personal information.

4.6 Summary of 'As-is' analysis

The current legislative landscape for the use of health information in Ireland draws on a number of discrete pieces of legislation making the practical application difficult to understand and navigate. There is a need for specific legislation and related guidance on the collection, use and sharing of health information that builds on existing legislation to promote appropriate and effective use.

Legislation and related guidance must encompass uses for both direct care and beyond direct care, and must be relevant for current and future requirements for health information. There needs to be improved clarity on what activities constitute the use of information for direct care and beyond direct care, and where exemptions for explicit consent may apply. These should be clearly communicated to health and social care professionals and the public so that there is clarity around rights and responsibilities.

While there are some governance structures in place, there is a need for enhanced governance structures for health information to cover additional uses of health information. This is particularly important as plans for eHealth initiatives advance and health and social care becomes more integrated, which will increase the potential for the collection, use and sharing of health information.

Despite recent progress in the area of eHealth, there is potential for improvement. There is a need for a more comprehensive infrastructure that would allow implementation of a future consent model. The citizen health portal, as proposed in Sláintecare, may provide the appropriate infrastructure. This would allow for greater transparency and individual control which would enable individuals to exercise their rights in relation to the use of their health information.

Consideration is also needed on how best to address the infrastructure gap in relation to the secure sharing and linkage of health information. Findings from the DASSL model study should be explored to examine the feasibility and suitability of implementing this model for use of health information beyond research, such as for management and planning of health and social care services.

The importance of public engagement has been acknowledged in the Sláintecare Implementation Strategy and Action Plan 2021-2023. The recent national public engagement on health information further develops understanding in this area. It will be important that engagement is continued over time to build and maintain a trusted relationship with the public to support successful implementation of changes or initiatives and realise the benefits from the use and sharing of health information.

5. International evidence on the collection, use and sharing of health information

5.1 Legislation

This section provides an overview of the relevant legislation adopted by each jurisdiction to define the 'rules' for the collection, use and sharing of health information. A detailed description of relevant legislation is outlined in Appendix 4.

In each of the eight jurisdictions examined in this review, a different approach has been taken to developing legislation in this area. Some have included detailed provisions for health information in data protection legislation or various health acts. In other jurisdictions, specific legislation and associated guidance has been developed to define the rules for the collection, use and sharing of health information. A summary of the legislative approaches adopted by jurisdictions is presented in this section and categorised into: general information legislation, health legislation, health information legislation and other arrangements.

5.1.1 General information legislation

All jurisdictions included in the review have data protection or privacy legislation in place. Each European jurisdiction is also governed by the GDPR.[7] 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.[7] In line with the GDPR, health data is identified as a special category of data in each European jurisdiction due to its sensitivity. In all jurisdictions included in the review, data protection legislation is used as the basis for all data processing; however, the provisions and details specific to health information vary. For example, in Denmark, the Data Protection Act (2018) outlines certain uses of health information beyond direct care which are exempt from requiring individual consent.[67] These include the use of information for statistical purposes if it is considered of significant societal importance; the use of information by an authority to carry out necessary supervisory and control tasks; and the use of information to evaluate a doctor's, dentist's or midwife's treatment efforts or as evidence of acquired qualifications in a training course.

5.1.2 Health legislation

All jurisdictions reviewed have included provisions for health information in associated health acts. In particular, the health acts generally include details regarding the collection, use and sharing of health information for direct care. For example, the Health and Social Care Act in England 2012 places a duty to share information between professionals for the provision of health services or adult social care.[68] Similarly, Estonia's Health Services Organization Act 2001 outlines that health information may be shared for the provision of care without explicit consent once principles of confidentiality are maintained.[20]

5.1.3 Health information legislation

As well as the provisions for health information in data protection and health legislation, there has also been a move towards developing specific legislation for health information. From the jurisdictions reviewed, the health information legislation has been developed in the areas of: health information privacy legislation, EHRs and the secondary use of information.

5.1.3.1 Health information privacy legislation

Some regions in Canada and Australia have introduced specific health information privacy legislation. In 2000, Ontario (Canada) enacted a health information privacy legislation, the Personal Health Information Protection Act (PHIPA).[27] This establishes a set of very clear and detailed rules regarding the collection, use and disclosure of personal health information. It provides a basis for practices and procedures which approved organisations, known as prescribed entities, must have in place to maintain the confidentiality of personal health information it receives and to protect the privacy of individuals. Those practices and procedures must be approved by the Information and Privacy Commissioner of Ontario every three years.

5.1.3.2 Electronic health records (EHRs)

Australia and Finland developed specific legislation to define the collection, use and sharing of information within their EHR. In 2012, Australia passed the My Health Records Act which set up the basis for the country's EHR (My Health Record).[69] In 2018, an amendment to the Act was passed which included a framework to guide the 'secondary uses' of data collected through My Health Records.[70] This aspect of the legislation describes the governance mechanisms and technical processes to be implemented before data can be released for research, policy and planning purposes.

5.1.3.3 Use of information beyond direct care

Finland is the only country included in the international review to introduce specific legislation to define the appropriate use of information for beyond direct care. In 2019, Finland passed the Act on the Secondary Use of Health and Social Data.[29] The approach taken by Finland to developing this specific legislation data builds on Australia's framework to guide the secondary use of My Health Record system data, as detailed above under electronic health records.

Example: Act on the Secondary Use of Health and Social Data, Finland

The **Act on the Secondary Use of Health and Social Data** facilitates the effective and safe processing of, and access to, personal health information for the following purposes: scientific research; statistics; development and innovation activities; steering and supervision of authorities; planning and reporting duties by authorities; teaching; and knowledge management. The Act also outlines the role of 'Findata' as a Data Permit Authority which issues permits for the secondary use of health data when data from several different controllers are combined, data originates from private health and social care service providers, and when data is saved in the EHR. Findata also acts as an intermediary service. Under the Act it has the remit to collate data from multiple sources and datasets and to link and de-identify information, before transferring it through a secure platform to the end-user.

The Act clearly sets out the different conditions associated with each of the permitted uses. For example, a data permit must be obtained from Findata for the secondary use of information for scientific research, statistics, education and the planning and reporting duties of an authority. For development and innovation activities, a request may be submitted to Findata to generate aggregated statistics but the activity must be related to either of the following: promote public health and social security; develop health and social care services and system; or protect the health and wellbeing of individuals. A data permit is not required for the use of information for knowledge management or the steering and supervision of authorities if the information being used has been generated by or is stored in the provider's registers. If additional information from other providers is required for comparison, the provider may apply to Findata to generate relevant aggregated statistics.

5.1.4 Other arrangements

In the absence of specific legislation to define the collection, use and sharing of all health information, some jurisdictions have developed national agreements or codes of practice to govern the collection, use and sharing of health information. For example, Australia established the National Health Information Agreement in 2013 to coordinate the development, collection and dissemination of all health information in Australia.[71]

New Zealand, Northern Ireland and the UK have introduced codes of practice to govern health information. The codes of practice for the use of health information are mandated through data protection or health legislation. In 2019, Northern Ireland introduced a *'Code of Practice on Protecting the Confidentiality of Service User Information'* to support and guide all those involved in health and social care regarding decisions about the protection, use and disclosure of service user information.[28] In 2020, New Zealand published the *'Health Information Privacy Code'* which sets out particular rules for

agencies in the health sector on the collection, use, storage and disclosure of health information by health agencies.[21] In 2021, the Information Commissioner in the UK also introduced a statutory Data Sharing Code of Practice to guide information management practices; this code of practice is relevant to all sectors.[72]

5.2 Governance structures for health information

International evidence suggests that jurisdictions with a mature and well-functioning health information system have strong national leadership, governance and management with clear organisational responsibility for managing health information systems. In comparison to other EU and OECD countries, Ireland has poor health information infrastructure and governance, fragmented practices, and limited capabilities for using health information beyond direct care.[57,58]

All jurisdictions reviewed have provisions within data protection legislation for the regulation of health information by the relevant commissioner. This could be either the privacy, data or information commissioner. In Denmark, the Danish Data Protection Agency (Datatilsynet) is the national monitoring authority, and monitors whether health information is used and shared in compliance with GDPR and the Danish Data Protection Act.[73] Appendix 4 outlines examples of where governance structures for the collection, use and sharing of health information are outlined in legislation.

In many jurisdictions, responsibility for the governance and management of health information is assigned to one or more specific agencies or organisations. In Australia, England, Estonia, Finland and New Zealand, there are key organisations that govern either all or the majority of national health and social care data collections and provide the strategic framework for the governance of these systems. Jurisdictions that have specific health information legislation in place outline how the use of health information should be governed; specifically for how health information can be used beyond direct care.

In Finland, a Data Permit Authority (Findata), was established to facilitate access to pseudonmyised information for research and statistics, teaching purposes, and planning and reporting duties, in line with conditions set out in relevant legislation, the Act on the Secondary Use of Health Information.[74] The Minister for Social Affairs and Health is responsible for appointing a steering committee and chairperson every three years for Findata. The Ministry for Social Affairs and Health and the steering committee are also responsible for establishing high-level expert groups to develop guidelines in relation to health information and security, and to support the operations of Findata. The membership of the steering committee and expert groups is outlined in legislation.

Additionally, robust governance structures exist for eHealth programmes in some jurisdictions, such as Denmark and Ontario (Canada).[75,76] Governance of eHealth programmes is well-structured with appropriate boards, groups and committees established. There is an emphasis on stakeholder engagement and communication

between the various, boards and groups. They have clear roles and responsibilities and have a wide-ranging remit, with good reporting structures in place.[3] The example below outlines the governance structures in place in Ontario (Canada) and the role of the Canadian Institute for Health Information (CIHI).

Example: Canadian Institute for Health Information, Ontario (Canada)

The **Canadian Institute for Health Information (CIHI)** is an independent, not-for-profit organisation that provides essential information on Canada's health systems and the health of Canadians. CIHI was established in 1994 by agreement between the federal, provincial and territorial governments of Canada.

Under Ontario's health privacy legislation, the Personal Health Information Protection Act (PHIPA), CIHI has a mandate to collect health information from various sources including hospitals, long-term care homes and regional health authorities, without explicit consent, for the purpose of analysis or compiling statistical information in relation to the management and planning of healthcare services. CIHI also facilitates access to health data, including linked data, for researchers and other health and social care professionals.

CIHI has a comprehensive Privacy Programme that governs the privacy and security of the personal health information that they hold. Under the PHIPA legislation, the procedures in place to maintain information confidentiality must be approved by the **Information and Privacy Commissioner of Ontario** every three years.

The CIHI Privacy Programme includes:

- a privacy and legal services department committed to developing a culture of privacy at CIHI
- an active Privacy, Confidentiality and Security Committee that includes representation from across the organisation
- a Chief Privacy Advisor who provides advice and counsel on privacy matters
- a Governance and Privacy Committee of the Board of Directors.

In some jurisdictions, a specific agency is assigned responsibility for managing the sharing of information and applying de-identification techniques. This facilitates the effective use of information beyond direct care while safeguarding privacy by operating in a regulated environment that meets security standards. Examples include Findata (Finland),[74] CIHI (Ontario, Canada),[77] and the Australian Digital Health Agency (Australia).[78] The Australian Digital Health Agency is the system operator for the EHR, 'My Health Record', and is responsible for preparing and providing de-identified data for research or public health purposes.[11] The governance of the use of information from the My Health Record system is outlined in the My Health Record Act.[69] The Australian

Institute of Health and Welfare is the data custodian and has an advisory role under the legislation.[79] The Secondary Use of Data Governance Board oversees development and operation of all secondary use infrastructure, and assessing applications for data use including monitoring processes to ensure that data is only used for approved purposes. In other jurisdictions, such as England, a number of agencies are involved in the coordination of this process with each assigned a specific responsibility. Further details on the English approach is provided below.

Example: NHS Digital and NHSX, England

In England, the **National Health Service (NHS) Digital**, has been assigned responsibility to manage the collection, use and sharing of health information. **NHS Digital** provides digital services for the NHS and social care, including the management of large health informatics programmes.

NHS Digital is also the national collator of health information, including national comparative information for uses beyond direct care; this is developed from the long-running hospital episode statistics which can help local decision-makers to improve the quality and efficiency of health and social care. The Department of Health and Social Care, NHS England and NHS Improvement come together under **NHSX** to drive digital transformation and lead policy, implementation and change.

NHS Digital Spine, a core IT infrastructure, has been developed which connects health and social organisations, and allows health information to be shared securely through national services, such as electronic prescribing service, summary care records and a GP practice transfer system. It also underpins the 'Secondary Uses Service' which is a repository for health information which enables a range of population health initiatives that include payment, public health planning and policy development.

In some jurisdictions, such as England and Northern Ireland, structures have been put in place to support the use and protection of health information across health and social care services. In England, the National Data Guardian (NDG) was established to provide advice and ensure personal information is used appropriately; it is supported by an expert panel. The NDG maintains the Caldicott Principles, which should underpin the use of personal health information to ensure confidentiality and appropriate use.[80] The Health and Social Care (National Data Guardian) Act 2018 placed the NDG on a statutory footing, granting it power to issue official guidance about the use and sharing of health information.[25] As well as the advisory role played by the NDG, there is also an established network of Caldicott Guardians. A Caldicott Guardian is responsible for protecting the confidentiality of health information in an organisation and making sure it is used appropriately.[81] All National Health Service (NHS) organisations and local authorities which provide health and social care services must have a Caldicott Guardian.

The aim of the network is to assist and guide in developing consistent standards and guidance for the use of information at a service level. The UK Caldicott Guardian Council (UKCGC) is the national body for Caldicott Guardians and operates as a sub-group of the NDG expert panel.[82] The UKCGC is also responsible for encouraging consistent standards and training, as well as developing guidance and policies relating to the Caldicott principles.

In Northern Ireland, Personal Data Guardians (PDGs) are responsible for ensuring high standards of confidentiality and security of service user information within an organisation. They act as a reference point for staff members who are unsure about their responsibility in relation to the sharing of information.[83] Each Health and Social Care Trust has a PDG in place.[83] The Privacy Advisory Committee was established in 2006 and is responsible for providing advice on consent and confidentiality matters, considering current and new uses of personal information and authorising such uses taking account of the legal and ethical issues surrounding privacy and confidentiality.[84] The Privacy Advisory Committee supports the network of PDGs in ensuring that the information governance standards outlined in the Code of Practice on Protecting the Confidentiality of Service User Information are maintained by all organisations providing health and social care.[28]

5.3 eHealth initiatives

An overview of eHealth developments in each jurisdiction is outlined in Appendix 5. All jurisdictions included in the review have implemented a unique national health identifier. eHealth infrastructure is well advanced in Australia, Estonia, Finland and Denmark with all of the following in place: national health identifier, EHRs, ePrescribing, eReferral and patient or health portals. Estonia has implemented additional features, including eConsultation and eAmbulance. Ontario (Canada) also has advanced eHealth infrastructure in place. However, currently, people do not have digital access to their own EHR but can request a printed copy of the information from their records.

England, New Zealand and Northern Ireland have a number of eHealth initiatives in place such as ePrescribing and other initiatives to capture important health information in the absence of an EHR:

- **England – Summary Care Records**: electronic record of important patient information, created from GP medical records.
- **New Zealand – Shared Care Record:** contains information on medical conditions, allergies, recalls, immunisations, recent test results and prescription medication.
- **Northern Ireland – Electronic Care Record (NIECR)**: captures information about an individual's medical history such as allergies, long-term health conditions, medication, lab tests, X-rays, referrals, investigation requests, appointments and discharge letters from various health or social care settings.

- **Northern Ireland – Key Information Summary (KIS) records**: includes details on medical history, agencies involved with the patient, list of care plans, preferred treatment arrangements, resuscitation status and advanced decision to refuse any treatments. The GP will decide if a person with a long-term illness or condition requires this record.

5.4 Consent model

5.4.1 Use of information for direct care

In all jurisdictions reviewed, and in Irish and EU legislation, the processing of personal health information is lawful for the provision of care. This means that health and social care professionals can collect, use and share personal information to provide safe and effective care to individuals without the need for explicit consent.

The importance of transparency is emphasised in legislation and related guidance or policy documents, and care professionals are obliged to inform individuals how their health information is used and shared. Some jurisdictions have explicit rules regarding the transparency of the use and sharing of this information. For example, the code of practices produced by Northern Ireland and New Zealand state that individuals must be fully and openly informed as to why the information is being collected and how it will be used and shared.[21,28] In New Zealand, the entire health and social care system has a shared responsibility to ensure individuals are sufficiently informed, and different approaches are taken to bring about greater transparency in this area.

However, jurisdictions have different approaches to categorising what constitutes the use of information for direct care. For example, in England and Northern Ireland, the use of information for direct care includes clinical audits and case reviews as these are viewed as sufficiently connected to the provision of direct care.[28,85] In England, the use of personal information for clinical audit is permissible within an organisation if it is carried out by a healthcare professional with a legitimate care relationship with the patient (one where they are involved in informing and or delivering direct care to an individual); in this scenario, explicit consent is not required.[85] For clinical audits across organisations, the use of personal information without consent is permissible where there is approval by a research ethics committee under Regulation 5 (decision procedure for research applications) of the Health Service (Control of Patient Information) Regulations 2002.[86]

While explicit consent is not required for the use of information for direct care, some jurisdictions provide individuals with an element of control over how their personal information is shared. For example, in Australia,[87] Estonia,[88] and Ontario (Canada),[27] individuals can request that some of their health records are not viewed, used and shared by healthcare professionals without their consent. Further details are provided in the box below. 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 their EHR, meaning that certain information will be blocked on the record and can only be accessed once access has been granted by the individual or in an emergency. In some jurisdictions where fully-integrated EHRs are in place, individuals can typically choose to control access to their personal information through an online portal.

Example: Control measures for the use of health information for direct care in Australia and Estonia

Australia

People can choose to opt-out of having an EHR **(My Health Record)** at any time through a patient portal. When an individual cancels a **My Health Record**, all information in the record, including any backups, is permanently deleted from the system and cannot be recovered. It will no longer be available to the individual or their healthcare providers, including in an emergency. People can set a **Record Access Code** which needs to be given to their health professional to access their records. Within **My Health Record**, people can decide which healthcare organisations can access their record and can restrict access to specific information.

Estonia

Explicit consent is not required to create an EHR but individuals can control the use of their personal information in their EHR. They can restrict access to certain information on their EHR, deny certain healthcare professionals access to all of their information, and grant access to other people, such as family members. These changes can be applied through an individual's online patient portal or via application to a healthcare provider or the Ministry of Social Affairs. People can also see, via the portal, who has accessed their EHR which supports transparency of information sharing. There is strict regulation of EHR access and serious professional implications if an EHR has been accessed inappropriately.

5.4.2 Use of information beyond direct care

In all jurisdictions, the approach taken to the use of personal health information beyond direct care is to seek explicit consent, with specific exemptions. The exemptions generally include: 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.

Information that is no longer identifiable is also typically exempt from the need to obtain explicit consent as it is no longer considered personal information. Under GDPR, specific techniques need to be employed to ensure it is irreversibly and effectively anonymised.(7) In New Zealand, the Health Information Governance Guidelines outline the specific data that must be removed in order for information to be considered anonymised.(89) In all jurisdictions, there are requirements in place that anonymised information should be used where possible, and personal information should only be used when necessary. Personal health information can be used for health research if explicit consent has been obtained or if permission has been granted by a research ethics board or similar entity, such as a data permit authority.

5.4.2.1 Structures to support use of information beyond direct care

Each jurisdiction has specific structures in place to manage and support the safe and effective use of health information for reasons beyond direct care. In Estonia, personal health information can be used for reasons beyond direct care without consent if a permit has been issued by the Data Protection Inspectorate.(30) In some jurisdictions, specific agencies are assigned with the responsibility of managing the use of information beyond direct care. These agencies have a specific role in managing information requests and have specific expertise in the latest anonymisation and data linkage techniques. Examples include Findata (Finland) (74) and CIHI (Ontario, Canada).(77)

Example: Findata, Finland

In **Finland**, personal health information can be used without consent for health services management, and the steering and supervision of health and social care authorities; the use of anonymised or pseudonymised information is recommended where possible. Aggregate data can be used to inform development and innovation activities. Applications must be made to **Findata**, the data permit authority, to use personal information for the purposes of scientific research and statistics, education and the planning and reporting duty of an authority. If a data permit application is successful, **Findata** will gather data from the relevant sources and use appropriate data linkage and de-identification techniques before sharing the anonymised or aggregate data with the applicant. This operates in a regulated environment as data will only be disclosed to an operating environment that meets particular conditions and data security standards which are approved by an independent data security assessment body. All of the permitted uses and associated conditions are detailed in the **Act on the Secondary Use of Health Information**.

Additional technical infrastructure is in place in these jurisdictions to enable the effective use of information beyond direct care and to manage the processing of large volumes of information in a highly secure and regulated environment. Advanced frameworks for the use of information beyond direct care include a system to collate data from multiple sources and datasets, technologies to analyse such datasets, and the capacity to link and de-identify information, before transferring it through a secure platform to the end-user. An example of such a model is Findata in Finland.[74] The presence of suitable technical infrastructure, within appropriate governance structures, ensures that data and information can be shared securely.

Example: Research Machine (Forskermaskinen), Denmark

In **Denmark,** public authorities can process personal health information without explicit consent from the individual. The secondary use of personal health information by other organisations requires the approval of an authority, depending on where the information is derived from; data processing registers must be maintained by the data controller and the data processor. Within certain conditions, personal information can be shared, either in a safe environment on the **Research Machine (Forskermaskinen)** or by ordering information extractions which are delivered in a secure environment.

5.4.2.2 Measures to support individual control for reasons beyond direct care

Similar to the approach taken for the use of information for direct care, some jurisdictions allow individuals to control how their information is used and shared beyond their direct care. The approaches taken, and the activities which an individual can opt-out of having their information used for, vary between jurisdictions. A number of jurisdictions, including Australia, England and Estonia, have moved to a dynamic opt-out model where individuals can change permissions for the use of their personal information for different purposes over time. In Australia, individuals can opt-out of de-identified information from their My Health Record being shared for public health and research purposes.[90] Personal health information from the My Health Record will never be released without explicit consent. In England, individuals can control whether their personal health information collected by the NHS is used for research and planning. Their personal information might still be used in some situations where there is an overriding public benefit, such as management of infectious diseases; when required by law; and when identifying information is removed.[91] In most cases, the infrastructure to enable people to control the use and sharing of their information beyond direct care is delivered through a online health portal, with the exception of England which has a separate online platform.

Example: Opt-out model for the use of information beyond direct care, England

In 2018, the **National Data Guardian** published ***'Health and Care – Review of Data Security, Consent and Opt-Outs'***. This review proposed a new consent opt-out model which would give people a clear choice about how their personal health information is used for purposes beyond their direct care. It resulted in the implementation of a national opt-out policy that allows individuals to opt-out of their personal health information being used for research and planning; this includes information that is collected by all NHS organisations, trusts and local authorities (including GP surgeries), as well as private organisations that provide NHS-funded care. If individuals choose to stop their personal health information being used for research and planning, it may still be used in certain situations; these situations include official national statistics, when there is an overriding public interest, when required by law, and when identifying information is removed. An online service is available where people can view or change their opt-out choice at any time. Since 2020, it is mandatory for all health and social care organisations to be compliant with the national opt-out policy.

5.5 Public engagement

Public engagement has been an important element in the successful implementation of eHealth solutions internationally. Engaging with the public in different formats is viewed as an important step to understanding their expectations and attitudes in relation to the use of their health information. For example, in Estonia, public engagement and trust building have been viewed as core components from the beginning of their eHealth journey.[92] Continued engagement with the public, healthcare professionals and organisations is considered essential to understanding and addressing concerns, and to supporting the continued success of eHealth initiatives. Table 3 outlines examples of public engagement initiatives across the jurisdictions included in the review.

Table 3. Examples of public engagement initiatives

Country	Key organisation	Method of engagement	Reason for engagement (inform, involve, consult, collaborate)
Australia	**Collaboration (Department of Health, Primary Health Networks, state health Departments and services) –** My Health Record engagement, 2016. [18]	▪ Trials of different participation arrangements for My Health Record. ▪ Independent evaluation of the trials by Siggins Miller Consultants.	**Consult**: To understand consumer reaction to different participation arrangements, as well as healthcare provider usage and upload of clinical information to the patients' record. To examine which model of consent resulted in greater participation.
Denmark	**Danish Ministry of Health –** engagement as part of 2018-2022 digital health strategy. [75]	▪ Patient as an active partner campaign.	**Inform and Involve:** To help patients to obtain better insight into their own illness and better use of their health data.
England	**National Data Guardian (NDG) –** helps to ensure that citizens' confidential information is safeguarded securely and used properly.[12]	Ongoing engagement: ▪ Citizens' juries ▪ Public dialogue through roundtable discussions ▪ Consultation workshops ▪ Stakeholder interviews ▪ Surveys.	**Collaborate:** To guide use of health information and policy.[93,94] Recommended new opt-out model and closure of the care.data programme which failed due to a lack of appropriate public engagement.
	Understanding Patient Data – explains how and why data can be used for care and research and how personal confidential information is kept safe.[95]	Ongoing engagement: ▪ Disseminate evidence through paper and webinars ▪ Focus groups/interviews ▪ Citizens' juries ▪ Surveys ▪ Public deliberation- citizen's summit (One London) ▪ One London report on public expectations of use of data.	**Collaborate:** To influence policy decisions and promote better public engagement around the use of their data.
Estonia	**Estonian Government –** public relations for eHealth initiatives.[92]	▪ Held discussions in areas of public relations, legal and ethics, and education ▪ Come Along! Campaign 2010.	**Inform and Consult:** Pre-implementation of EHR engagement led to greater understanding on needs and built trust from the onset. Continued engagement to build digital literacy sessions targeting 100,000 citizens.
Finland	**Ministry for Foreign Affairs, Department for Communications**- This is Finland. [96]	▪ 'Data is good' Social media campaign targeted towards patient and professionals.	**Inform and Consult:** To highlight the benefits of healthcare data — campaign ran for 100 days and focused on publishing the benefits of health data.

Country	Key organisation	Method of engagement	Reason for engagement (inform, involve, consult, collaborate)
New Zealand	**New Zealand Government –** Data Futures Partnership- Our Data, Our Way. [97]	▪ Large public survey ▪ Public meetings.	**Consult:** To test people's preferences and tolerance for data sharing and use, and to examine the measures that need to be in place for them to be comfortable sharing their data.
	Social Investment Agency – Data Protection and Use Policy engagement. [98,99]	▪ Social assembly (n=83) – >1000 service users participated ▪ Report 'What you told us'.	**Inform:** To inform policy and to educate public on what's appropriate, what's not, and how to keep data safe.
	Ministry of Health – National health information platform. [100]	▪ Consulted with over 70 consumers and whānau, and health professionals.	**Inform and Involve:** To inform new health information platform and understand the challenges.
Northern Ireland	**Health and Social Care Northern Ireland –** engagement prior to launching NIECR in and when consent model changed in 2019.[101,102]	▪ Household leaflet drop ▪ Information on website ▪ Leaflets and posters ▪ Social media promotion ▪ Press release and press events ▪ Training to clinicians ▪ Information included with all medical cards issued ▪ Telephone enquiry service.	**Inform:** To make patients, service users and the public aware of how data would be shared and the change in the consent model.
Ontario (Canada)	**Canada Health Infoway –** Connecting Patients for Better Health report, 2018.[103]	▪ Public opinion surveys ▪ Workshops- Better Health Together through digital solutions.	**Consult:** To understand public's perspectives and understand needs. To create the Citizens' Vision for Better Health by understanding perspectives and experiences with digital health.

5.5.1 Key organisations responsible

In general, engagement is undertaken or commissioned by government or health services agencies. However, in England, organisations have been established with the specific purpose of promoting effective and safe use of health information. The NDG was established in 2014 to act as a champion for patients and the public on matters relating to confidential health information; in 2018, it gained statutory powers to issue official guidance about the processing of health and adult social care data.[25] In addition, Understanding Patient Data was established with the unique purpose of helping the public understand how their health information is or can be used.[95] This organisation has also assisted in promoting public engagement in the area of health information and influencing decisions in relation to policy and practice.

5.5.2 Approach to engagement

As outlined in Table 3, a range of public engagement methods are being used in different jurisdictions including:

- one-way communication to inform the public of changes or new initiatives by circulating leaflets, posters and placing information on websites;
- consulting with and involving the public in decision-making through workshops and interviews where facilitators get the opportunity to listen, learn and discuss experiences and views;
- collaborating with the public through active participation activities, such as citizen juries, and ongoing consultations to achieve a deep understanding of needs and desires of the public.

It appears that an ongoing public engagement process that incorporates different methods of engagement is most effective at supporting the successful implementation of new eHealth initiatives or changes in the collection, use and sharing of health information. In England, the focus on extensive public engagement on health information emerged after 'care.data', a national database of patient interactions with the healthcare system, failed in 2013 due to a lack of engagement with the public regarding the establishment of the national database.[104] This prompted the development of Understanding Patient Data which, along with the NDG, works to build public awareness in this area while also capturing people's views, expectations and concerns about information use. It then communicates these views to shape relevant policy and legislation.[95] However, despite this history, in 2021 the Department of Health and Social Care had to pause the implementation of a new framework for data extraction called the General Practice Data for Planning and Research (GP-DPR) collection.[105,106] It emerged that there had been a lack of appropriate engagement and flexibility regarding dynamic consent procedures, and the public voiced their concerns. To remedy this, the National Data Guardian and Understanding Patient Data have advised a need for meaningful consultation regarding the GP-DPR and use of patient data generally.

A number of positive examples of extensive engagement include the work undertaken in New Zealand through the 'Data Futures Partnership – Our Data, Our Way'.[97] This engagement was established to inform the development of guidelines which public and private organisations can use to develop a 'social licence'. A social licence is "when people trust that their data will be used as they have agreed, and accept that enough value will be created, [and] they are likely to be more comfortable with its use".[107] The national engagement aimed to test people's preferences and examine the measures that would make them more comfortable in relation to the use and sharing of their information. The initiative was developed and implemented to enable a broad cross-section of New Zealanders to easily express their personal positions on a range of hypothetical data scenarios. It found that in order for people to feel comfortable about a proposed information use, they want to be fully informed and be active partners in

decisions about the collection, use and sharing of their information. The national engagement process took place over a six-week period, but it is seen as a single step in building a social licence and that ongoing engagement is crucial to building and maintaining public trust.

5.6 Summary of international evidence

Legislation

- The approaches adopted by jurisdictions to developing legislation for health information differs. A number of jurisdictions, including Australia, Finland, New Zealand, Northern Ireland and Ontario (Canada), have specific legislation and codes of practice in place to regulate the collection, use and sharing of health information. This demonstrates a need to clearly define rules for the use of health information, both for direct care and beyond direct care.
- Specifically, the approach taken by Australia and Finland to develop legislation and mandated frameworks for the use of information beyond direct care highlights the importance of defining structures to use and share large volumes of information effectively in a regulated and controlled environment.
- In countries with advanced eHealth models, there is either specific legislation or provisions made within related legislation to define the collection, use and sharing of information for digital health records, such as the My Health Records Act in Australia or the Health Act in Denmark. As health information becomes increasingly digitalised, these laws are vital to ensure information is collected, used and shared appropriately in line with public expectations and requirements.

Governance structures

- Jurisdictions with a mature and well-functioning health information system have strong national leadership, governance and management with clear organisational responsibility for managing health information systems.
- All jurisdictions reviewed have made provisions within data protection legislation for the regulation of health information by the relevant commissioner.
- Jurisdictions with specific health information legislation have more detailed governance structures outlined, particularly for the use of information beyond direct care. In some jurisdictions, the responsibility for the governance and management of the majority of national health and social care data collections is assigned to one or more specific agencies or organisations.
- Within these arrangements, a specific agency is assigned responsibility for managing data requests and applying linking and anonymisation techniques, for example in Australia and Finland. This facilitates the effective use of

information beyond direct care while safeguarding privacy by operating in a regulated environment that meets data security standards.

Consent – Use for direct care

- In each jurisdiction, the collection, use and sharing of personal health information for the provision of care does not require explicit consent.
- In England and Northern Ireland, the use of data for direct care includes clinical audit and case review as this is viewed as an integral aspect of the provision of safe and effective care.
- The importance of transparency is emphasised in legislation where healthcare professionals are obliged to inform the individual about how their health information may be used and shared. Some jurisdictions have explicit rules regarding the transparency of the use and sharing of this information.
- Some jurisdictions provide individuals with an element of control over how their personal information is shared. For example, individuals can request that some of their health records are not viewed, used and shared by healthcare professionals without their consent. Individuals are usually informed of the impact that this may have on their direct care.
- In some jurisdictions, where fully-integrated EHRs are in place, individuals can choose to control access to their health information through an online portal.

Consent – Use beyond direct care

- In all jurisdictions, the approach taken to the use of personal health information beyond direct care is to seek explicit consent, with specific exemptions. Exemptions generally include: 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. Information that is no longer identifiable is also typically exempt.
- Personal health information can be used for health research if explicit consent has been obtained or if permission has been granted by a research ethics board or similar entity, such as a data permit authority.
- Some jurisdictions allow individuals to control how their information is used and shared beyond their direct care, although the options over which people have control differs between jurisdictions. In Australia, individuals can opt out of de-identified information from their My Health Record being shared and personal health information will never be shared without explicit consent. In England, individuals can control if personal health information is used for research and planning, but it might still be used where there is an overriding public benefit or required by law.

Public engagement

- Public engagement is generally undertaken or commissioned by governments or health services agencies, primarily when they are implementing change to data processing or developing a new system. In England, organisations have been established with the specific purpose of promoting effective and safe use of patient data, which have assisted in promoting public engagement in this area and influencing policy decisions.
- Public engagement is carried out for a variety of reasons, depending on the maturity of the engagement levels, to include: informing the public of a new initiative or the benefits of sharing in a controlled manner; consulting and involving individuals 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 and how best they may be incorporated into decision-making.
- Greater levels of public engagement can lead to increasing public trust and better understanding of the benefits of using health information appropriately.
- Continued public engagement, that is authentic and employs different methods to ensure all voices are engaged, is considered essential to understanding expectations and addressing concerns, and to supporting the continued success of eHealth initiatives.

6. Conclusion

The information garnered from this evidence synthesis, alongside feedback from stakeholders (through the Advisory Group, the National Public Engagement on Health Information and international stakeholders), will inform the recommendations for a consent model on the collection, use and sharing of health information in Ireland. 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. However, to support the consent model and to deliver the requirements and governance structures, a strategic approach is needed to ensure that personal information is processed safely and securely in line with individual's preferences. An examination of the current situation in Ireland identified a number of examples of good practice. In addition, the Sláintecare Implementation Strategy and Action Plan 2021-2023 outline further areas for eHealth advancement.[52] There are, however, many opportunities for improvement, especially when Ireland is compared with its international counterparts.

A recent position paper published by HIQA called for reform of Ireland's national health information system and recommended developing a health information strategy that takes a holistic and cohesive approach to the collection, use and sharing of health information for both direct care and reasons beyond direct care, across public and private healthcare.[3] 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.[3,57,58] The OECD report, 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.[3,57]

In Ireland, there is no clear legislative framework for the use of health information. In addition, there is a lack of agreed definitions in relation to health information and what constitutes use for direct care and beyond direct care. The current legislative landscape 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 differ 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 need to clearly define rules for the processing of health information.

When a legislative framework is available, including clear guidance on the rules for the collection, use and sharing of health information, professionals have the knowledge and confidence to share personal information in the best interest of patients and the public. However, in the absence of such laws, regulation and guidance, data and information are not used to their full potential. In addition, it is important to establish appropriate data

governance structures and the technical infrastructure to promote and encourage the optimal and safe use of information for wider public benefit. For example, the establishment of Findata as the data permit authority in Finland offers an excellent example of good practice. Findata facilitates the effective use of information beyond direct care while safeguarding privacy by operating in a highly regulated and controlled environment.

New legislation and related guidance for health information should comprehensively cover the different uses of health information and offer clear guidance as to how, and when, information can be shared. It must also be relevant for current and future modes of collecting, using and sharing health information in line with advances in eHealth initiatives and digital health technologies.

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.

Glossary of abbreviations

Abbreviation	Explanation
CIHI	Canadian Institute for Health Information
CSO	Central Statistics Office
DASSL	Data Access Storage Sharing and Linkage
DPO	Data Protection Officer
EHR	Electronic Health Record
EU	European Union
GDPR	General Data Protection Legislation
GP	General Practitioner
GP-DPR	General Practice Data for Planning and Research
HIPS	Health Information and Patient Safety
HIQA	Health Information and Quality Authority
HPSC	Health Protection Surveillance Centre
HRB	Health Research Board
HRCDC	Health Research Consent Declaration Committee
HSE	Health Service Executive
IAP2	International Association of Public Participation
ICGP	Irish College of General Practitioners
ICT	Information and Communications Technology
IHI	Individual health identifier
IPPOSI	Irish Platform for Patient Organisations, Science & Industry
KIS	Key Information Summary
NCP	National Contact Point
NCRI	National Cancer Registry Ireland
NDG	National Data Guardian
NHS	National Health Service
ODGB	Open Data Governance Board
OECD	Organisation for Economic Co-operation and Development
PDG	Personal Data Guardians
PHIPA	Personal Health Information Protection Act
RDGB	Research Data Governance Board
SCR	Shared Care Record
UKCGC	United Kingdom Caldicott Guardian Council
WHO	World Health Organization

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 has 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 electronic health record, 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 healtheducation, 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.[(2)]

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 electronic health records, 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 and or 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): a complete digital record of a patient's journey, throughout their life, across all health and social care settings, for every patient. 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.

Shared care record: a record that enables health and social care providers in different settings to view health records with the individual's consent or their representative's consent, where appropriate. It brings together information from various systems into a single place for care professionals to use to support the delivery of care.

Summary care record: a summary of the main parts of a person's health record that will be most useful to a healthcare professional providing care to an individual at a different location to usual (for example, on holiday, visiting friends or in an emergency).

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. 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.

3. 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.

4. 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.

5. 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.

6. 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.

7. General Data Protection Legislation 2016 (European Union). Available from: https://gdpr-info.eu/. 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. 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.].

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

12. 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.

13. 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.

14. 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.

15. 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.

16. 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.

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

18. 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.

19. 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.

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

21. 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.

22. Privacy Act 1988 (Australia). Available from: https://www.legislation.gov.au/Details/C2014C00076. Accessed on: 29 October 2021.

23. Australian Institute of Health and Welfare Act 1987 (Australia). Available from: https://www.legislation.gov.au/Details/C2016C01008. Accessed on: 29 October 2021.

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

25. 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.

26. 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.

27. 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.

28. 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.

29. 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.

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

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

32. Statistics Act 1993 (Ireland). Available from: https://www.irishstatutebook.ie/eli/1993/act/21/enacted/en/html#:~:text=%20%20%20Number%2021%20of%201993%20,%20%20%20%2015%20more%20rows%20. Accessed on: 29 October 2021.

33. Civil Registration Act 2004 (Ireland). Available from: https://www.irishstatutebook.ie/eli/2004/act/3/enacted/en/html. Accessed on: 29 October 2021.

34. European Union (Measures for a High Common Level of Security of Network and Information Systems) Regulations 2018 Available from: https://www.irishstatutebook.ie/eli/2018/si/360/made/en/print. Accessed on: 29 October 2021.

35. Data Sharing and Governance Act 2019 (Ireland). Available from: https://www.irishstatutebook.ie/eli/2019/act/5/enacted/en/html. Accessed on: 29 October 2021.

36. European Union (Open Data and Re-use of Public Sector Information) Regulations 2021 Available from: https://www.irishstatutebook.ie/eli/2021/si/376/made/en/print. Accessed on: 29 October 2021.

37. Health Act 1947 (Ireland). Available from: https://www.irishstatutebook.ie/eli/1947/act/28/enacted/en/html. Accessed on: 29 October 2021.

38. Health Act 1953 (Ireland). Available from: https://www.irishstatutebook.ie/eli/1953/act/26/enacted/en/html#:~:text=%20%20%20Number%2026%20of%201953.%20,%20%20%20%209%20more%20rows%20. Accessed on: 29 October 2021.

39. Health (Duties of Officers) Order 1949 (Ireland). Available from: https://www.irishstatutebook.ie/eli/1949/si/128/made/en/print#:~:text=HEALTH%20%28DUTIES%20OF%20OFFICERS%29%20ORDER%2C%201949.%20The%20Minister,hereby%20declares%20and%20orders%20as%20follows%20%3A%E2%80%94%201. Accessed on: 29 October 2021.

40. Infectious Disease Regulations 1981 (Ireland). Available from: https://www.irishstatutebook.ie/eli/1981/si/390/made/en/print. Accessed on: 29 October 2021.

41. Medicinal Products (Prescription and Control of Supply) Regulations 2003 (Ireland). Available from: https://www.irishstatutebook.ie/eli/2003/si/540/made/en/print. Accessed on: 29 October 2021.

42. Misuse of Drugs Regulations 2017 (Ireland). Available from: https://www.irishstatutebook.ie/eli/2017/si/173/made/en/print. Accessed on: 29 October 2021.

43. The Health (Provision of Information) Act 1997 (Ireland). Available from: https://www.irishstatutebook.ie/eli/1997/act/9/enacted/en/html#:~:text=HEALTH%20%28PROVISION%20OF%20INFORMATION%29%20ACT%2C%201997%20AN%20ACT,BE%20IT%20ENACTED%20BY%20THE%20OIREACHTAS%20AS%20FOLLOWS%3A. Accessed on: 29 October 2021.

44. Health Identifiers Act 2014 (Ireland). Available from: https://www.irishstatutebook.ie/eli/2014/act/15/enacted/en/html. Accessed on: 29 October 2021.

45. Cross-Border Directive 2011/24 (European Union). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32011L0024. Accessed on: 29 October 2021.

46. Health Information and Patient Safety Bill (Ireland) Available from: https://assets.gov.ie/11441/ce1d167063254135a89e72aa7a96c728.pdf. Accessed on: 29 October 2021.

47. Patient Safety (Notifiable Safety Incidents) Bill 2019 (Ireland). Available from: https://www.gov.ie/en/publication/9e2562-patient-safety-bill/#:~:text=The%20Patient%20Safety%20%28Notifiable%20Patient%20Safety%20Incidents%29%20Bill,to%20go%20through%20the%20process%20of%20becoming%20law. Accessed on: 29 October 2021.

48. 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.

49. 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.

50. 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.

51. Terrés, AM., Cole, N., O'Hanlon, D., O'Hara, MC. , Dever, S. *Governance of research in the HSE and HSE funded healthcare services - A scoping report*. Dublin: 2019. Available from: https://hseresearch.ie/wp-content/uploads/2020/05/Governance-of-Research-in-the-HSE-and-HSE-Funded-Healthcare-Services.-A-Scoping-Report-compressed.pdf. Accessed on: 29 October 2021.

52. 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.

53. Irish Government Department of Health. *Sláintecare Implementation Strategy*. Dublin: 2019. Available from: https://assets.gov.ie/9914/3b6c2faf7ba34bb1a0e854cfa3f9b5ea.pdf. Accessed on: 29 October 2021.

54. Health Service Executive. *GP Electronic Referral - Background Information* [Online]. Available from https://www.hse.ie/eng/services/list/5/cancer/profinfo/resources/gpelectronic/gp%20electronic%20referral%20-%20background%20information.html. Accessed on: 29 October 2021.

55. European Commission. *Communication on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society*. 2018. Available from: https://digital-strategy.ec.europa.eu/en/library/communication-enabling-digital-transformation-health-and-care-digital-single-market-empowering. Accessed on: 29 October 2021.

56. National Statistics Board. *Quality Information for All – Numbers Matter. National Statistics Board Strategic Priorities for Official Statistics*. Dublin: 2021. Available from: https://www.nsb.ie/media/nsbie/pdfdocs/NSB_Statement_of_Strategy_2021_2026.pdf. Accessed on: 29 October 2021.

57. 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.

58. 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.

59. 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.

60. 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.

61. Irish Medical Council. *Guide to Professional Conduct and Ethics for Registered Medical Professionals*. 2018. Available from: https://www.medicalcouncil.ie/news-and-publications/reports/guide-to-professional-conduct-ethics-8th-edition.html. Accessed on: 29 October 2021.

62. Irish College of General Practitioners Data Protection Working Group. *Processing of Patient Personal Data: A Guideline for General Practitioners v2.3*. Dublin: 2019. Available from: https://www.icgp.ie/speck/properties/asset/asset.cfm?type=Document&id=07BFBD54-DBE7-4EF3-8A60D884D2AA4EE7&property=document&filename=GP_GDPR_Guideline_v2_3..pdf&revision=tip&mimetype=application%2Fpdf&app=icgp&disposition=inline. Accessed on: 29 October 2021.

63. Stockdale, J., Cassell, J. , Ford, E. . Giving something back?: A systematic review and ethical enquiry into public views on the use of patient data for research in the United Kingdom and the Republic of Ireland. *Wellcome Open Research*. 2019; 3(6).

64. Irish Platform for Patient Organisations, Science and Industry (IPPOSI). *Citizens' Jury on Health Information* [Online]. Available from https://www.ipposi.ie/our-work/policy/health-information/citizens-jury/. Accessed on: 3 November 2021.

65. 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.

66. 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.

67. Data Protection Act 2018 (Denmark). Available from: https://www.datatilsynet.dk/media/6894/danish-data-protection-act.pdf. Accessed on: 29 October 2021.

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

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

70. My Health Records Amendment (Strengthening Privacy) Act 2018 (Australia). Available from: https://www.legislation.gov.au/Details/C2018A00154#:~:text=%20My%20Health%20Records%20Amendment%20%28Strengthening%20Privacy%29%20Act,that%20the%20System%20Operator%20has%20a...%20More%20. Accessed on: 29 October 2021.

71. National Health Information Agreement 2013 (Australia). Available from: https://meteor.aihw.gov.au/content/index.phtml/itemId/182135#:~:text=The%20National%20Health%20Information%20Agreement%20%28NHIA%29%20is%20an,the%20Australian%20Government%20and%20state%2Fterritory%20government%20health%20authorities. Accessed on: 29 October 2021.

72. United Kingdom Information Commissioner's Office. *Data Sharing Code of Practice*. London: 2021. Available from: https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf. Accessed on: 29 October 2021.

73. Datatilsynet. *Danish Data Protection Agency* [Online]. Available from https://www.datatilsynet.dk/english/. Accessed on: 29 October 2021.

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

75. 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.

76. 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.

77. *Canadian Institute for Health Information* [Online]. Available from https://www.cihi.ca/en. Accessed on: 3 November 2021.

78. *Australian Digital Health Agency* [Online]. Available from https://www.digitalhealth.gov.au/. Accessed on: 29 October 2021.

79. 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.

80. 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.

81. The National Data Guardian. *Guidance about the appointment of Caldicott Guardians, their role and responsibilities*. London: 2021. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1013756/Caldicott_Guardian_guidance_v1.0_27.08.21.pdf. Accessed on: 29 October 2021.

82. 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.

83. Privacy Advisory Committee. *Confidentiality of Service User Information - Guidance for all staff working in health and social care in Northern Ireland*. 2012. Available from: http://www.privacyadvisorycommittee.hscni.net/staff-guidance-on-confidentiality_March%202012.pdf. Accessed on: 1 November 2021.

84. Privacy Advisory Committee. *Privacy Advisory Committee – Terms of Reference* 2006. Available from: http://www.privacyadvisorycommittee.hscni.net/PAC%20Terms%20of%20Reference_July%202006.pdf Accessed on: 1 November 2021.

85. Health and Social Care (Safety and Quality) Act 2015 (England). Available from: https://www.legislation.gov.uk/ukpga/2015/28/pdfs/ukpga_20150028_en.pdf. Accessed on: 29 October 2021.

86. The Health Service (Control of Patient Information) Regulations 2002 (England). Available from: https://www.legislation.gov.uk/uksi/2002/1438/contents/made. Accessed on: 2 November 2021.

87. 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.

88. 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.

89. New Zealand Ministry of Health. *Health Information Governance Guidelines*. Wellington: 2017. Available from: https://www.health.govt.nz/publication/hiso-100642017-health-information-governance-guidelines. Accessed on: 29 October 2021.

90. 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.

91. 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.

92. Estonian Government. *Estonian eHealth Strategic Development Plan 2020*. 2015. Available from: https://www.sm.ee/sites/default/files/content-editors/sisekomm/e-tervise_strateegia_2020_15_en1.pdf. Accessed on: 29 October 2021.

93. Hopkins , H., Kinsella, S., Evans, G. , Reid, S. *Putting Good into Practice. A public dialogue on making public benefit assessments when using health and care data*. London: 2021. Available from: https://www.scie-socialcareonline.org.uk/putting-good-into-practice-a-public-dialogue-on-making-public-benefit-assessments-when-using-health-and-care-data/r/a116f00000UuYHMAA3. Accessed on: 29 October 2021.

94. United Kingdom Government Department of Health. *Information: To share or not to share? The Information Governance Review*. London: 2013. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf. Accessed on: 29 October 2021.

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

96. Finnish Toolbox. *This is Finland*. 2019. Available from: https://toolbox.finland.fi/wp-content/uploads/sites/2/2019/08/jun2019_tif_social_media_campaign.pdf Accessed on: 29 October 2021.

97. Data Futures Partnership. *Our Data, Our Way. What New Zealand people expect from guidelines for data use and sharing. Findings from public engagement* Wellington: 2017. Available from: http://hiqasrv2116.hiqa.local/MM.NET/Stub.aspx?MID=13209306&AID=6513520&ASig=214A83D22D20ACCF209736966D7D397970E6C650&AName=b3VyLWRhdGEtb3VyLXdheS1maW5hbC1yZXBvcnQucGRm&Ver=5. Accessed on: 2 November 2021.

98. Social Investment Agency. *What you told us - Findings of the 'Your voice, your data, your say' engagement on social wellbeing and the protection and use of data*. Wellington: 2018. Available from: https://swa.govt.nz/assets/Uploads/what-you-told-us.pdf. Accessed on: 2 November 2021.

99. Social Investment Agency. *From listening to learning*. Wellington: 2018. Available from: https://swa.govt.nz/assets/Uploads/From-Listening-to-Learning.pdf. Accessed on: 2 November 2021.

100. New Zealand Ministry of Health. *Hira (National health information platform)* [Online]. Available from https://www.health.govt.nz/our-work/digital-health/other-digital-health-initiatives/hira-national-health-information-platform. Accessed on: 2 November 2021.

101. *Personal communication with Mary McCluskey, Head of eHealth Projects, NIECR.* 2019.

102. *Privacy Advisory Committee, Northern Ireland.* [Online]. Available from http://www.privacyadvisorycommittee.hscni.net/. Accessed on: 1 November 2021.

103. Canada Health Infoway. *Connecting Patients for Better Health*. 2018. Available from: https://www.infoway-inforoute.ca/en/component/edocman/3564-connecting-patients-for-better-health-2018/view-document?Itemid=0. Accessed on: 29 October 2021.

104. 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.

105. NHS Digital. *General Practice Data for Planning and Research (GPDPR)* [Online]. Available from https://digital.nhs.uk/data-and-information/data-collections-and-data-sets/data-collections/general-practice-data-for-planning-and-research. Accessed on: 1 November 2021.

106. Understanding Patient Data. *Trustworthy use of GP data: what must happen now* [Online]. Available from https://understandingpatientdata.org.uk/news/trustworthy-use-gp-data-what-must-happen-now. Accessed on: 1 November 2021.

107. Data Futures Partnership. *A Path to Social Licence - Guidelines for Trusted Data Use*. 2017. Available from: https://www.aisp.upenn.edu/wp-content/uploads/2019/08/Trusted-Data-Use_2017.pdf. Accessed on: 1 November 2021.

108. Sundhedsloven (Danish Health Care Act 2010). Available from: https://www.mindbank.info/item/1194. Accessed on: 2 November 2021.

109. *The Electronic Processing of Customer Data in Social Welfare and Health Care Act 2007 (Finland)*. Available from: https://www.finlex.fi/fi/laki/ajantasa/2007/20070159. Accessed on: 3 November 2021.

110. Decree of the Ministry of Social Affairs and Health on Patient Documents 2009. Available from: https://www.finlex.fi/fi/laki/alkup/2009/20090298. Accessed on: 3 November 2021.

111. Act on the status and rights of patients, (1992). Available from: https://www.finlex.fi/en/laki/kaannokset/1992/en19920785.pdf. Accessed on: 2 November 2021.

112. Privacy Act 2020 (New Zealand). Available from: https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html. Accessed on: 2 November 2021.

113. Health Act 1956 (amended) (New Zealand). Available from: https://legislation.govt.nz/act/public/1956/0065/latest/whole.html. Accessed on: 2 November 2021.

114. Data Availability and Transparency Bill 2020 (Australia). Available from: https://www.legislation.gov.au/Details/C2020B00199. Accessed on: 2 November 2021.

115. Research Ethics Review of Health Research Projects Act 2018 (Denmark). Available from: https://en.nvk.dk/rules-and-guidelines/act-on-research-ethics-review-of-health-research-projects. Accessed on: 2 November 2021.

116. The Health Service (Control of Patient Information) Regulations 2002 (United Kingdom). Available from: https://www.legislation.gov.uk/uksi/2002/1438/regulation/3/made. Accessed on: 2 November 2021.

117. Cybersecurity Act 2018 (Estonia). Available from: https://www.riigiteataja.ee/en/eli/523052018003/consolide. Accessed on: 2 November 2021.

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

119. Health Care Act 2010 (Finland). Available from: https://www.finlex.fi/fi/laki/kaannokset/2010/en20101326.pdf. Accessed on: 2 November 2021.

120. Electronic Prescribing Act 2021 (Finland). Available from: https://www.kanta.fi/en/notice/-/asset_publisher/cf6QCnduV1x6/content/stm-sosiaalihuollon-palvelunantajille-velvoite-liitty%C3%A4-kanta-palveluihin-uusi-asiakastietolaki-voimaan-1.11.2021. Accessed on: 2 November 2021.

121. Public Health and Disability Act 2000 (New Zealand). Available from: https://www.legislation.govt.nz/act/public/2000/0091/latest/DLM80051.html. Accessed on: 2 November 2021.

122. Privacy Act 1985 (Canada). Available from: https://laws-lois.justice.gc.ca/eng/acts/p-21/FullText.html. Accessed on: 2 November 2021.

123. 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.

124. Municipal Freedom of Information and Protection of Privacy Act 1990 (Canada). Available from: https://www.canlii.org/en/on/laws/stat/rso-1990-c-m56/latest/rso-1990-c-m56.html. Accessed on: 3 November 2021.

125. The People's Health Care Act 2019 (Canada). Available from: https://www.ola.org/en/legislative-business/bills/parliament-42/session-1/bill-74. Accessed on: 3 November 2021.

Appendices

Appendix 1: Definitions of health information

Country	Definition	Source
Australia	Health information defined as: a) Information or an opinion about: i. the health (at any time) of an individual; or ii. an individual's expressed wishes about the future provision of healthcare; or iii. healthcare provided, or to be provided, to an individual; that is also personal information; or b) other personal information collected to provide, or in providing, healthcare; or c) other personal information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances; or d) genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual. Information concerning a person includes: (i) a reference to information as to the whereabouts, existence or non-existence of a document concerning a person; and (ii) a reference to information identifying a person or body providing information concerning a person.	Privacy Act 1988 [22] Australian Institute of Health and Welfare Act 1987 [23]
Denmark	Health information is not specifically defined but when discussing health information the following is outlined: the patient's health conditions, other purely private matters and other confidential information in connection with the treatment of the patient. Personal data: Any information or data relating to an identified or identifiable natural person.	The Danish Act of Health 2010 (Sundhedloven)[108] Data Protection Act 2018 [67]
England	"Health and adult social care data" means information (however recorded) that—(a) relates to—(i) the physical or mental health or condition of an individual, the diagnosis of his or her condition or his or her care or treatment; (ii) adult social care provided to an individual (or an assessment for such care); (iii) adult carer support provided to an individual (or an assessment for such support), whether or not the identity of the individual is ascertainable, or (b) is to any extent derived, directly or indirectly, from such information. Personal data: Any information relating to an identified or identifiable living individual.	Health and Social Care (National Data Guardian) Act 2018 [25] Data Protection Act 2018 [24]
Estonia	No definition of personal health information. Legislation focuses on personal data required for the provision of a health service, data relating to the state of health of a data subject, and data related to healthcare.	Health Services Organisation Act 2001 [20]
Finland	Customer data refers to personal data (as laid out in Data Protection Act) that must be kept secret by law and that is stored in a customer register or an associated administrative register as a result of social and healthcare customership or for processing of benefits.	Secondary Use of Health and Social Data Act 2019 [29]

	Patient data means information concerning a patient which is included in a patient document as referred to in the Patients Act [documents or technical records used, drawn up or arrived when the treatment of the patient is arranged and carried out and which contain information on his/her state of health or otherwise personal information about the patient].	Act on Electronic Processing of Social and Health Care Customer Data 2007 (109)
New Zealand	Health information, in relation to an identifiable individual, means— (a) information about the health of that individual, including their medical history; or (b) information about any disabilities that individual has, or has had; or (c) information about any health services or disability services that are being provided, or have been provided, to that individual; or (d) information provided by that individual in connection with the donation, by that individual, of any body part or any bodily substance of that individual or derived from the testing or examination of any body part, or any bodily substance of that individual; or (e) information about that individual which is collected before or in the course of, and incidental to, the provision of any health service or disability service to that individual.	Health Information Privacy Code 2020 (21)
Northern Ireland	Information means— (a) information (however recorded) which relates to the physical or mental health or condition of an individual, to the diagnosis of an individual's condition or to the care or treatment of an individual, (b) information (however recorded) which relates to the social well-being of an individual or to the care of, or assistance to, an individual, and (c) information (however recorded) which is to any extent derived, directly or indirectly, from such information, whether or not the identity of the individual in question is ascertainable from the information.	Health and Social Care (Control of Data Processing) Act (Northern Ireland) 2016 (26)
Ontario (Canada)	Personal health information: Identifying information about an individual in oral or recorded form, if the information, (a) relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family, (b) relates to the providing of health care to the individual, including the identification of a person as a provider of health care to the individual, (c) is a plan of service within the meaning of the Home Care and Community Services Act, 1994 for the individual, (d) relates to payments or eligibility for health care, or eligibility for coverage for health care, in respect of the individual, (e) relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any such body part or bodily substance, (f) is the individual's health number, or (g) identifies an individual's substitute decision-maker.	Personal Health Information Privacy Act (PHIPA) 2020 (27)

Appendix 2: Uses of health information for direct care

Country	Definition/Description	Source
Australia	(Simplified outline) Health information may be collected, used and disclosed from a healthcare recipient's My Health Record for the purpose of providing healthcare to the recipient, subject to any access controls set by the recipient (or if none are set, default access controls). A participant in the My Health Record system is authorised to collect, use and disclose health information included in a registered healthcare recipient's My Health Record if the collection, use or disclosure of the health information is: (a) for the purpose of providing healthcare to the registered healthcare recipient; and (b) in accordance with: (i) the access controls set by the registered healthcare recipient; or (ii) if the registered healthcare recipient has not set access controls—the default access controls specified by the My Health Records Rules or, if the My Health Records Rules do not specify default access controls, by the System Operator. Does not authorise a participant in the My Health Record system to collect, use or disclose health information included in healthcare recipient-only notes. A participant in the My Health Record system is authorised to disclose health information included in a registered healthcare recipient's My Health Record for any purpose if the disclosure of the health information is: (a) to the registered healthcare recipient's nominated representative; and (b) in accordance with: (i) the access controls set by the registered healthcare recipient; or (ii) if the healthcare recipient has not set access controls—the default access controls specified by the My Health Records Rules or, if the My Health Records Rules do not specify default access controls, by the System Operator. A participant in the My Health Record system is authorised to collect, use and disclose health information included in a registered healthcare recipient's My Health Record if: (a) the participant reasonably believes that: (i) the collection, use or disclosure is necessary to lessen or prevent a serious threat to an individual's life, health or safety; and (ii) it is unreasonable or impracticable to obtain the healthcare recipient's consent to the collection, use or disclosure; and (b) unless the participant is the System Operator—the participant advises the System Operator of the matters in paragraph (a); and (c) the collection, use or disclosure occurs not later than five days after that advice is given.	My Health Records Act 2012 [69]
	A permitted health situation exists in relation to the collection by an organisation of health information about an individual if: (a) the information is necessary to provide a health service to the individual; and (b) either: (i) the collection is required or authorised by or under an Australian law (other than this Act); or (ii) the information is collected in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation.	Privacy Act 1988 [22]

	A permitted health situation exists in relation to the disclosure by an organisation of health information about an individual if: (a) the organisation provides a health service to the individual; and (b) the recipient of the information is a responsible person for the individual; and (c) the individual: (i) is physically or legally incapable of giving consent to the disclosure; or (ii) physically cannot communicate consent to the disclosure; and (d) another individual (the carer) providing the health service for the organisation is satisfied that either: (i) the disclosure is necessary to provide appropriate care or treatment of the individual; (ii) the disclosure is made for compassionate reasons; and (e) the disclosure is not contrary to any wish: (i) expressed by the individual before the individual became unable to give or communicate consent; and (ii) of which the carer is aware, or of which the carer could reasonably be expected to be aware; and (f) the disclosure is limited to the extent reasonable and necessary for a purpose mentioned in paragraph (d).	
Denmark	With the patient's consent, healthcare professionals may pass on information to other healthcare professionals about the patient's health conditions, other purely private matters and other confidential information in connection with the treatment of the patient or treatment of other patients. Information may be shared without patient's consent where 1) it is necessary for the sake of a current course of treatment for the patient, and the transfer takes place taking into account the patient's interest and needs, 2) the transfer includes a discharge letter from a doctor employed in the hospital system to the patient's general practitioner or the general practitioner who has referred the patient for hospital treatment, 3) the transfer includes a discharge letter from a doctor employed at a privately owned hospital, clinic, etc., to the doctors mentioned in no. 2, when the treatment has been provided by agreement with a regional council or a municipal council in accordance with this Act, (4) the disclosure is necessary for the legitimate protection of an obvious public interest or of essential interests for the patient, including a patient who is unable to take care of his own interests, the healthcare professional or others; 5) the transfer is made to the patient's general practitioner by a doctor who acts as his deputy, 6) the transfer takes place to a doctor, dentist or midwife about a patient that the recipient has previously participated in the treatment of, when (a) the transfer is necessary and relevant for use in evaluating the recipient's own efforts in the treatment or as evidence of acquired qualifications in a training course; and (b) the transfer takes into account the patient's interests and needs; or 7) the transfer takes place to a student who, as part of a health science or health professional education, participates in the treatment of a patient without being an assistant when (a) the disclosure is necessary for the student's understanding of the treatment situation or the evaluation of the student's participation in the treatment situation; and b) the transfer takes place taking into account the patient's interest and needs.	The Danish Act of Health 2010 (Sundhedloven) (108)

England	Duty to share information applies in relation to information about an individual that is held by a relevant health or adult social care commissioner or provider. The relevant person must ensure that the information is disclosed to— (a) persons working for the relevant person, and (b) any other relevant health or adult social care commissioner or provider with whom the relevant person communicates about the individual; applies only so far as the relevant person considers that the disclosure is— (a) likely to facilitate the provision to the individual of health services or adult social care in England, and (b) in the individual's best interests. The relevant person need not comply with subsection (2) if the relevant person reasonably considers that one or more of the following apply— (a) the individual objects, or would be likely to object, to the disclosure of the information; (b) the information concerns, or is connected with, the provision of health services or adult social care by an anonymous access provider; (c) for any other reason the relevant person is not reasonably able, or should not be required, to comply.	Health and Social Care (Safety and Quality) Act 2015 (85)
Estonia	Healthcare providers have the right to process personal data required for the provision of a health service including sensitive personal data, without the permission of the data subject.	Health Services Organisation Act 2001 (20)
Finland	The primary purpose of personal data refers to the purpose for which the personal data was originally saved. Participants in patient care or related tasks may only process patient records to the extent required by their job duties and responsibilities. The access rights of those working in the healthcare unit to the information contained in the patient records must be defined in detail. A healthcare professional or other person working in or performing tasks in a healthcare unit shall not provide a third party with information contained in patient records without the written consent of the patient. A third party means persons other than those involved in the care of a patient or related tasks in the relevant functional unit or on its behalf.	Secondary Use of Health and Social Data Act 2019 (29) Decree of the Ministry of Social Affairs and Health on patient records 2009 (110) The Law Regarding the Status and Rights of a Patient 1992 (111)
New Zealand	An agency that holds personal information that was obtained in connection with one purpose may not use the information for any other purpose unless the agency believes, on reasonable grounds that the purpose for which the information is to be used is directly related to the purpose in connection with which the information was obtained.	Privacy Act 2020 (112)
Northern Ireland	The use and disclosure of personal identifiable information is for the direct care of that service user. Service users must be informed in a manner appropriate to their communication needs of what information sharing is necessary for their care and the likely extent of the sharing for a particular episode of care. They should be informed about the necessary involvement of a range of administrative staff who support professional staff. Provided service users are adequately informed in this way, express consent is not necessary and	Code of Practice on Protecting the Confidentiality of Service User Information, 2019 (28)

	their consent to the disclosure of information necessary for their care may be inferred from their acceptance of that care In emergency situations, uses or disclosures may be made, but only the minimum necessary information should be used or disclosed to deal with the emergency situation. Reasonable care should be taken not to override any relevant legally binding wishes of the service user which have been expressed in advance of the situation arising. As soon as possible after disclosure, the service user should be told what information has been disclosed and their consent sought for any necessary further disclosures. Review of care, including clinical audit and case review carried out by members of the care team and those supporting them, is for the purpose of improving the direct care of that service user. Such purposes have sufficient connection with that direct care for the sharing of information during the review of care to be justified on the basis of implied consent, provided the individual has been informed.	
Ontario (Canada)	A health information custodian may use personal health information about an individual: where information can be used for the purpose for which the information was collected or created and for all the functions reasonably necessary for carrying out that purpose, but not if the information was collected with the consent of the individual, or the information to be collected is reasonably necessary for providing health care or assisting in providing health care to the individual and it is not reasonably possible to collect, directly from the individual and the individual expressly instructs otherwise.	Personal Health Information Privacy Act (PHIPA) 2020 [27]

Appendix 3: Uses of health information for beyond direct care

Country	Definition/Description	Source
Australia	A participant in the My Health Record system is authorised to collect, use and disclose health information included in a healthcare recipient's My Health Record if: (a) the collection, use or disclosure is undertaken for the purpose of the management or operation of the My Health Record system, if the healthcare recipient would reasonably expect the participant to collect, use or disclose the health information for that purpose; (b) the collection, use or disclosure is undertaken in response to a request by the System Operator for the purpose of performing a function or exercising a power of the System Operator; (c) the participant reasonably believes that the collection, use or disclosure by the participant is necessary to lessen or prevent a serious threat to public health or public safety; (d) the collection, use or disclosure is required or authorised by a Commonwealth, State or Territory law; (e) for purposes relating to the provision of indemnity cover for a healthcare provider; (f) a court or tribunal other than a coroner orders or directs the System Operator to disclose health information; (g) the System Operator: (i) has reason to suspect that unlawful activity that relates to the System Operator's functions has been, is being or may be engaged in; and (ii) reasonably believes that use or disclosure of the information is necessary for the purposes of an investigation of the matter or in reporting concerns to relevant persons or authorities. The following are prohibited purposes: (i) underwriting a contract of insurance that covers the healthcare recipient; or (ii) determining whether to enter into a contract of insurance that covers the healthcare recipient (whether alone or as a member of a class); or (iii) determining whether a contract of insurance covers the healthcare recipient in relation to a particular event; or (iv) an employer employing, or continuing or ceasing to employ, the healthcare recipient; (b) a purpose prescribed by the regulations. A permitted health situation exists in relation to the collection by an organisation of health information about an individual if: (a) the collection is necessary for any of the following purposes: (i) research relevant to public health or public safety; (ii) the compilation or analysis of statistics relevant to public health or public safety; (iii) the management, funding or monitoring of a health service; and (b) that purpose cannot be served by the collection of information about the individual that is de-identified information; and (c) it is impracticable for the organisation to obtain the individual's consent to the collection; and (d) any of the following apply: (i) the collection is required by or under an Australian law (other than this Act); (ii) the information is collected in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation; (iii) the information is collected in accordance with guidelines approved under the Act.	My Health Records Act 2012 [69] Privacy Act 1988 [22]
Denmark	With the patient's consent, authorised healthcare professionals may obtain electronic health information about the patient's health conditions, other purely private matters and other	The Danish Act of Health 2010 (Sundhedloven) [108]

	confidential information for purposes other than treatment. Electronic health information can be used without consent for the following purposes: 1) The collection is made by a doctor, dentist or midwife who has previously participated in the treatment of the patient, and (a) the acquisition is necessary and relevant for use in evaluating the doctor's, dentist's or midwife's own efforts in the treatment or as evidence of acquired qualifications in a training course; (b) the collection takes into account the interests and needs of the patient; and (c) the collection takes place immediately following the course of treatment and no later than 6 months after the end of the treatment by the collecting doctor, dentist or midwife or referral of the patient, unless the collection is required as part of the specialist or specialist dental education. 2) The collection is carried out by an authorized healthcare professional, and a) the collection is necessary in connection with quality assurance or development of treatment processes and workflows, (b) the processing of the information is of significant societal importance and takes place for statistical purposes, taking into account the patient's integrity and privacy; (c) the management of the place of treatment has, in accordance with specified criteria, given permission for the authorized healthcare professional in question to carry out the collection; (d) the information is recorded in the electronic systems of the place of processing in question less than 5 years prior to collection; and e) it is possible to subsequently identify that the collection has taken place for the purpose of quality assurance or development. 3) The collection is carried out by a healthcare professional or another person who is subject to a duty of confidentiality under the law and who is employed by the data controller for the information, and (a) the collection is necessary in connection with accreditation or follow-up of compliance with requirements from central health authorities for treatment in the health care system; (b) the management of the place of treatment or the central regional or municipal administrative management of the place of treatment has given permission for the person concerned to carry out the collection; and (c) it is possible to subsequently identify that the collection took place in connection with accreditation or follow-up on whether requirements from central health authorities for treatment in the health care system are met. Health information can be used without consent for the following purposes: 1) it follows from law or regulations laid down by law that the information must be passed on and the information must be assumed to have a significant effect on the receiving authority's case processing, 2) the disclosure is necessary for the legitimate pursuit of an obvious public interest or for essential reasons of the patient, the healthcare professional or others, 3) the transfer is necessary for an authority to carry out supervisory and control tasks, 4) the transfer takes place to an authority-approved accreditation body and is necessary for the purpose of documenting workflows for use in accreditation; or 5) the transfer takes place for the purpose of following up on an unintended event in the region, the municipality or a private hospital.	

England	Processing of information is possible if it is: considered necessary for health and social care purposes, such as (a) preventive or occupational medicine, (b) the assessment of the working capacity of an employee, (c) medical diagnosis, (d) the provision of health care or treatment, (e) the provision of social care, or (f) the management of health care systems or services or social care systems or services; (g) necessary for reasons of public interest in the area of public health, and is carried out— (i) by or under the responsibility of a health professional, or (ii) by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law; (h) of substantial public interest, such as equality of opportunity or treatment, support for individuals with a particular disability or medical condition, safeguarding of economic well-being of certain individuals, insurance, and occupational pensions.	Data Protection Act 2018 [24]
	Confidential patient information relating to patients referred for the diagnosis or treatment of neoplasia may be processed for medical purposes which comprise or include— (a) the surveillance and analysis of health and disease; (b) the monitoring and audit of health and health related care provision and outcomes where such provision has been made; (c) the planning and administration of the provision made for health and health related care; (d) medical research approved by research ethics committees; (e) the provision of information about individuals who have suffered from a particular disease or condition where— (i) that information supports an analysis of the risk of developing that disease or condition; and (ii) it is required for the counselling and support of a person who is concerned about the risk of developing that disease or condition. Confidential patient information may be processed with a view to— (a) diagnosing communicable diseases and other risks to public health; (b) recognising trends in such diseases and risks; (c) controlling and preventing the spread of such diseases and risks; (d) monitoring and managing— (i) outbreaks of communicable disease; (ii) incidents of exposure to communicable disease; (iii) the delivery, efficacy and safety of immunisation programmes; (iv) adverse reactions to vaccines and medicines; (v) risks of infection acquired from food or the environment (including water supplies); (vi) the giving of information to persons about the diagnosis of communicable disease and risks of acquiring such disease. Confidential patient information may be processed for medical purposes provided that the processing has been approved—(a) in the case of medical research, by [the Health Research Authority], and (b) in any other case, by the Secretary of State. The Health Research Authority may not give an approval unless a research ethics committee has approved the medical research concerned. So far as it is practical to do so, remove from the information any particulars which identify the person to whom it relates which are not required for the purposes for which it is, or is to be, processed; not allow any person access to that information other than a person who, by virtue of his contract of employment or otherwise, is involved in processing the information for one or more of those purposes and is aware of the purpose or purposes	Health Service (Control of Patient Information) Regulations 2002 [86]

	for which the information may be processed; ensure that appropriate technical and organisational measures are taken to prevent unauthorised processing of that information; review at intervals not exceeding 12 months the need to process confidential patient information and the extent to which it is practicable to reduce the confidential patient information which is being processed. No person shall process confidential patient information under these Regulations unless he is a health professional or a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.	
Estonia	In order to make the surveys, analyses and organise health statistics necessary for the management of health policy and performance of international obligations; access to the following personal data of a patient in the Health Information System in a way which does not enable the identification of a patient: 1) data on the person of a patient; 2) data on the health service provider; 3) data on in-patient health services; 4) data on out-patient health services, including day care; 5) data on diagnoses; 6) data on the indicators describing the state of health of a patient; 7) data on medicinal products; 8) data on performed operations, analyses, examinations and procedures. Personal data may be processed without the consent of the data subject for the needs of scientific and historical research and official statistics, in particular in a pseudonymised format or a format which provides equivalent level of protection. If scientific and historical research is based on special categories of personal data (health data), the ethics committee of the area concerned shall first verify compliance with the terms and conditions provided in legislation. Scientific research is deemed to also include any analyses and studies by executive power which are carried out for the purposes of policy development. In order to prepare these, the executive power has the rights to make queries to databases of another controller or processor and process the personal data received. The Estonian Data Protection Inspectorate shall verify, prior to the beginning of the specified processing of personal data, compliance with the terms and conditions provided in legislation.	Health Services Organisation Act 2001 (20) Data Protection Act 2018 (30)
Finland	Secondary purpose of personal data refers to the processing of personal data for a purpose other than the primary purpose. The secondary uses include: (a) statistics; (b) scientific research; (c) development and innovation activities [application and use of engineering and business data and other existing data together with personal data for the purpose of developing new or significantly improved products, processes, or services]; (d) education; (e) knowledge management [processing of data carried out by a service provider in their customer, service and production processes for the purpose of supporting operations, production, financial control, management and decision making]; (f) steering of social and healthcare by authorities [statutory steering of social and healthcare organisations by the national social and health care authorities based on personal data and statistics collected for the purpose or on data received for the steering or supervision task on a case-by-case basis]; (g) supervision of social and healthcare by authorities [statutory	Secondary Use of Health and Social Data Act 2019 (29)

	supervision of social and healthcare professionals and units by the national social and health care authorities]; (h) planning and reporting duty of an authority.	
New Zealand	Any person (being an agency that provides services or arranges the provision of services) may disclose health information— (a) if that information— (i) is required by any person specified in subsection (2) (ii) is required or is essential for the purpose set out in that subsection in relation to the person so specified; or (b) if that disclosure is permitted— (i) by or under a code of practice issued under the Privacy Act 2020; or (ii) if no such code of practice applies in relation to the information, by any of the information privacy principles set out in the Privacy Act 2020. Subsection (2): The persons and purposes referred to in subsection (1)(a) are as follows: (a) any medical officer of a prison within the meaning of the Corrections Act 2004, for the purposes of exercising or performing any of that person's powers, duties, or functions under that Act: (b) any probation officer within the meaning of the Corrections Act 2004, for the purposes of exercising or performing any of that person's powers, duties, or functions under any enactment: (c) a Social Worker or a Care and Protection Co-ordinator within the meaning of the Oranga Tamariki Act 1989, for the purposes of exercising or performing any of that person's powers, duties, or functions under that Act: (d) any employee of the department for the time being responsible for the administration of the Social Security Act 2018, for the purposes of administering sections 206 and 207 (factors affecting benefit: hospitalisation) of that Act: (e) any member of the New Zealand Defence Force, for the purposes of administering the Armed Forces Discipline Act 1971 or the Defence Act 1990: (f) any constable, for the purposes of exercising or performing any of that person's powers, duties, or functions: (g) any employee of the Ministry of Health, for the purposes of— (i) administering this Act or the Hospitals Act 1957; or (ii) compiling statistics for health purposes: (h) any employee of the Ministry of Agriculture and Forestry authorised by the chief executive of that Ministry to receive the information, for the purposes of administering the Meat Act 1981 or the Animal Products Act 1999: (i) any employee of the New Zealand Transport Agency, for statistical or research purposes in relation to road safety or the environment: (j) any employee of a district health board, for the purposes of exercising or performing any of that board's powers, duties, or functions under the New Zealand Public Health and Disability Act 2000. Notwithstanding any enactment, rule of law, or other obligation, any person may supply to any other person health information that does not enable the identification of the individual to whom the information relates. A health agency that holds health information must not disclose the information unless the agency believes, on reasonable grounds,— (a) that the disclosure is to— (i) the individual concerned; or (ii) the individual's representative where the individual is dead or is unable to exercise their rights under these rules; or (b) that the disclosure is authorised by— (i) the	Health Act 1956 (as amended) [113] Health Information Privacy Code 2020 [21]

	individual concerned; or (ii) the individual's representative where the individual is dead or is unable to give their authority under this rule; or (c) that the disclosure of the information is one of the purposes in connection with which the information was obtained; or (d) that the source of the information is a publicly available publication and that, in the circumstances of the case, it would not be unfair or unreasonable to disclose the information; or (e) that the information is information in general terms concerning the presence, location, and condition and progress of the patient in a hospital, on the day on which the information is disclosed, and the disclosure is not contrary to the express request of the individual or their representative; or (f) that the information to be disclosed concerns only the fact of death and the disclosure is by a health practitioner or by a person authorised by a health agency, to a person nominated by the individual concerned, or the individual's representative, partner, spouse, principal caregiver, next of kin, whānau, close relative, or other person whom it is reasonable in the circumstances to inform; or (g) that the information to be disclosed concerns only the fact that an individual is to be, or has been, released from compulsory status under the Mental Health (Compulsory Assessment and Treatment) Act 1992 and the disclosure is to the individual's principal caregiver. Compliance with subrule (b) is not necessary if the health agency believes on reasonable grounds, that it is either not desirable or not practicable to obtain authorisation from the individual concerned and— (a) that the disclosure of the information is directly related to one of the purposes in connection with which the information was obtained; or (b) that the information is disclosed by a health practitioner to a person nominated by the individual concerned or to the principal caregiver or a near relative of the individual concerned in accordance with recognised professional practice and the disclosure is not contrary to the express request of the individual or their representative; or (c) that the information— (i) is to be used in a form in which the individual concerned is not identified; or (ii) is to be used for statistical purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or (iii) is to be used for research purposes (for which approval by an ethics committee, if required, has been given) and will not be published in a form that could reasonably be expected to identify the individual concerned; or (d) that the disclosure of the information is necessary to prevent or lessen a serious threat to— (i) public health or public safety; or (ii) the life or health of the individual concerned or another individual; or (e) the disclosure of the information is necessary to enable an intelligence and security agency to perform any of its functions; or (f) that the disclosure of the information is essential to facilitate the sale or other disposition of a business as a going concern; or (g) that the information to be disclosed briefly describes only the nature of injuries of an individual sustained in an accident and that the individual's identity and the disclosure is— (i) by a person authorised by the person in charge of a hospital; and (ii) to a person authorised by the person in charge of a news entity; and for the purpose of publication or broadcast in connection with the news activities of that news entity and the disclosure is not contrary to the express request of the individual	

	concerned or their representative; or (h) that the disclosure of the information— (i) is required for the purpose of identifying whether an individual is suitable to be involved in health education and so that individuals so identified may be able to be contacted to seek their authority in accordance with subrule (1)(b); and (ii) is by a person authorised by the health agency to a person authorised by a health training institution; or (i) that the disclosure of the information— (i) is required for the purpose of a professionally recognised accreditation of a health or disability service; or (ii) is required for a professionally recognised external quality assurance programme; or (iii) is required for risk management assessment and the disclosure is solely to a person engaged by the agency for the purpose of assessing the agency's risk; and the information will not be published in a form which could reasonably be expected to identify any individual nor disclosed by the accreditation quality assurance or risk management organisation to third parties except as required by law; or (j) that non-compliance is necessary— (i) to avoid prejudice to the maintenance of the law by any public sector agency, including prejudice to the prevention, detection, investigation, prosecution and punishment of offences; or (ii) for the conduct of proceedings before any court or tribunal (being proceedings that have commenced or are reasonably in contemplation); or (k) that the individual concerned is or is likely to become dependent upon a controlled drug, prescription medicine, or restricted medicine and the disclosure is by a health practitioner to a Medical Officer of Health for the purposes of section 20 of the Misuse of Drugs Act 1975 or section 49A of the Medicines Act 1981.	
Northern Ireland	Secondary use defined as the use and disclosure of personal identifiable information for purposes of health and social care not directly related to care of that service user. Many uses of service user information are increasingly required for evidence-based practice and for a rational approach to health and social care service provision. The following are examples of such secondary uses: planning; financial management; commissioning of services; investigating complaints; auditing accounts; teaching; health and social care research; public health monitoring; registries; infectious disease reporting. If personal identifiable information is to be made available for secondary purposes, there must also be some clear public interest in making the information available, such as a clear benefit to service users or a clear general good (e.g. public safety). The possible exceptions to requirement for consent are where a statute, court or tribunal imposes a requirement to disclose or there is an overriding public interest in the use or disclosure. Consent is not required where there is a statutory obligation to disclose or a discretionary disclosure is justified in the public interest. All organisations seeking service user information for other than direct care should be seeking anonymised or pseudonymised data. The Health and Care Number (HCN) of service users should be used instead of usual patient identifiers such as name and	Code of Practice on Protecting the Confidentiality of Service User Information, 2019 [28]

	address.	
Ontario (Canada)	A health information custodian may use personal health information about an individual: (a) for planning or delivering programs or services that the custodian provides or that the custodian funds in whole or in part, allocating resources to any of them, evaluating or monitoring any of them or detecting, monitoring or preventing fraud or any unauthorized receipt of services or benefits related to any of them; (b) for the purpose of risk management, error management or for the purpose of activities to improve or maintain the quality of care or to improve or maintain the quality of any related programs or services of the custodian; (c) for educating agents to provide health care; (d) for the purpose of disposing of the information or modifying the information in order to conceal the identity of the individual; (e) for the purpose of seeking the individual's consent, or the consent of the individual's substitute decision-maker; (f) for the purpose of a proceeding or contemplated proceeding in which the custodian or the agent or former agent of the custodian is, or is expected to be, a party or witness, if the information relates to or is a matter in issue in the proceeding or contemplated proceeding; (g) for the purpose of obtaining payment or processing, monitoring, verifying or reimbursing claims for payment for the provision of health care or related goods and services; (h) for research conducted by the custodian if the custodian prepares a research plan and has a research ethics board approve it and for that purpose.	Personal Health Information Privacy Act (PHIPA) 2020 [27]
Ireland	Secondary purpose means (a) the promotion of patient safety, including clinical auditing and the investigation and reporting of patient safety incidents, (b) the identification or prevention of a threat to public health, (c) the management of health services, including— (i) the planning, monitoring, delivery, improvement, auditing and evaluation of health services, (ii) the investigation and resolution of complaints relating to health services, and (iii) the management of national health systems, (d) the carrying out of health research that is the subject of a research ethics approval (or any cognate expression) under an enactment or European act prescribed for the purposes of this paragraph, (e) the performance of any function conferred on a person under this Act or another enactment for which the processing of identifiers is necessary, (f) the provision of a scheme of health or health-related insurance operated by an undertaking authorised to so do under the Health Insurance Act 1994 , or (g) any— (i) processing of relevant information (individuals) required to protect or prevent injury or other damage to the health or safety of an individual, (ii) processing of relevant information (individuals) required by or under an enactment, rule of law or equity or order of a court, (iii) processing of relevant information (individuals) that is in accordance with the Data Protection Acts 1988 and 2003 and required for— (I) the purposes of obtaining legal advice, (II) the purposes of, or in the course of, legal proceedings, or (III) the purposes of, or in the course of, alternative dispute resolution procedures agreed between a service provider and an individual as a means of resolving a dispute, or (iv) subject to section 3 (4) and (8), processing of relevant information (individuals) relating to health that is prescribed for the purposes of this subparagraph.	Health Identifiers Act 2014 [44]

Appendix 4: Legislation outlining the governance of health information

Country	Data protection	Direct care	Beyond direct care	eHealth	Governance structures
Australia	**Privacy Act 1988** - specific section to define health information and uses of information. [22]	**Privacy Act, 1988 -** Health information is necessary to provide a health service to the individual.[22] **My Health Records Act, 2012 -** Health information may be collected, used and disclosed from a healthcare recipient's My Health Record for the purpose of providing healthcare to the recipient, subject to any access controls set by the recipient (or if none are set, default access controls).[69]	**Privacy Act, 1988 –** Information can be collected for (i) research relevant to public health or public safety; (ii) the compilation or analysis of statistics relevant to public health or public safety; (iii) the management, funding or monitoring of a health service. That purpose cannot be served by the collection of information about the individual that is de-identified information; and it is impracticable for the organisation to obtain the individual's consent to the collection.[22] **My Health Records Act, 2012-** The My Health Records Rules may, in accordance with section 109A, prescribe a framework to guide the collection, use and disclosure of de-identified data and, with the consent of healthcare recipients, health information, for research or public health purposes.[69]	**My Health Records Act, 2012** - establishment and operation of a voluntary national system for the provision of access to health information relating to recipients of healthcare.[69]	**Privacy Act, 1988 –** Australian Information Commission regulates the Privacy Act. Privacy Advisory Committee advises the Commissioner on relevant matters.[22] **Data Availability and Transparency Bill, 2020** National Data Commissioner is the regulator for the data sharing scheme. Entities must be accredited by the Commissioner in order to have public sector data shared with or through them. National Data Advisory Council function of advising the Commissioner.[114] **My Health Records Act, 2012-** Data Governance Board established to oversee the operation of the framework prescribed by My Health Records Rules.[69] **National Health Information Agreement -** Australian Health Ministers' Advisory Council (AHMAC) agree governance arrangements for information management. [71]
Denmark	**Data Protection Act 2018 –** Specific detail on processing of health information for treatment and management of care.[67]	**Health Act 2010 –** With the patient's consent, healthcare professionals may pass on information to other healthcare professionals about the patient's health conditions, other purely private matters and other confidential information in connection with the treatment of the patient or treatment of other patients.[108]	**Data Protection Act 2018 –** The processing of specific categories of personal data may be necessary in the public interest as regards public health without the consent of the data subject.[67] **Health Act 2010 –** specific detail and conditions outlined for 'disclosure of information etc. purposes other than treatment and for other purposes' (with patient's consent) – e.g. quality assurance, statistical purposes, healthcare management, public health, supervisory and control tasks, and accreditation. [108]	**Health Act 2010 –** includes detailed sections outlining conditions for the collection of electronic health information.[108]	**Data Protection Act 2018 –** consists of a Council and a Secretariat, is responsible for monitoring any processing operation covered by this Act, the General Data Protection Regulation and other legislation that falls within the scope of the Regulation's special rules on the processing of personal data. The Data Protection Agency shall carry out its functions with complete independence.[67] **Act on Research Ethics Review of Health Research Projects, 2018 –** legal framework for the research ethics evaluation of health research projects by the committees and the tasks of the committee system on this basis.[115]

Country	Data protection	Direct care	Beyond direct care	eHealth	Governance structures
			Act on Research Ethics Review of Health Research Projects, 2018 – details legal framework for governance of research projects and consent.[115]		
England	**UK Data Protection Act 2018 –** processing personal data for health or social care is carried out by or under the responsibility of a health professional or a social work professional or by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law.[24] **ICO data sharing code of practice –** developed under section 121 of the Data Protection Act 2018.[72]	**Health and Social Care Act 2012 & 2015 –** duty to share information for the provision of health services or adult social care in England, and also if in the individual's best interests.[68,85] **UK Data Protection Act 2018 –** processing of data for health or social care purposes, both for provision and management of care.[24]	**Data Protection Act 2018 –** processing for research and public health – necessary for reasons of public interest (when specific conditions apply).[24] **The Health Service (Control of Patient Information Regulations) 2002 –** provisions for confidential patient information to be processed without consent for public health, audit and monitoring of care, medical purposes including medical research.[116]	*No specific legislation for digital health services.*	**Data Protection Act 2018 –** Information Commissioner independently upholds the information rights of citizens in the UK, and is able to enforce sanctions where breaches of regulation occur.[24] **Health and Social Care (National Data Guardian) Act 2018 –** Data Guardian publishes guidance about the processing of health and adult social care data in England.[25]
Estonia	**Personal Data Protection Act 2018** - protection of persons for processing of personal data.[30]	**Health Services Organization Act 2001 -** Health care providers, who have the obligation to maintain confidentiality arising from law, have the right to process personal data required for the provision of a health service, including sensitive personal data, without the permission of the data subject.[20]	**Personal Data Protection Act 2018** - Personal data may be processed without the consent of the data subject for the needs of scientific and historical research and official statistic, in particular in a pseudonymised format or a format which provides equivalent level of protection.[30]	**Cybersecurity Act 2018** - requirements for the maintenance of network and information systems essential for the functioning of society and state and local authorities' network and information systems (includes healthcare).[117]	**Personal Data Protection Act 2018** - If scientific and historical research is based on special categories of personal data, the ethics committee of the area concerned shall first verify compliance with the terms and conditions provided for in this section. If there is no ethics committee in the scientific area, the compliance with the requirements shall be verified by the Estonian Data Protection Inspectorate.[30]
Finland	**Data Protection Act 2018 –** processing data for healthcare is identified as a special category of data.[118]	**Health Act 2010 –** includes provision for handling of patient data stating that medical records can be used and shared for provision of care without consent.[119] **Data Protection Act 2018 –** arranging or producing services processes data it has received in the context of these activities on the state of health or disability of a person or on the healthcare and rehabilitation services received by a person, or other data necessary for the treatment of the data subject.[118]	**Data Protection Act 2018 –** processing of data for scientific or historical research purposes or for statistical purposes.[118] **Secondary Use of Health and Social data Act 2019 –** to enable efficient and secure processing of personal data collection during the provision of social and health care as well as personal data collected for the purpose beyond direct care such as steering supervision, researching and collecting statistics, and also to enable personal data to be combined across 4 key national data collections.[29]	**Health Act 2010 –** Section 9 addresses handling of patient data in electronic record.[119] **Electronic Processing of Client Data in Social and Health Care Services 2007 –** public healthcare organisations are obliged to enter patient records in a nationally centralised archive.[109] **The Act on Electronic Prescription, 2021 –** mandatory introduction of electronic prescriptions.[120]	**Data Protection Act 2018 –** national supervisory authority referred to in the Data Protection Regulation is the Data Protection Ombudsman, who works under the auspices of the Ministry of Justice.[118] **Secondary Use of Health and Social data Act 2019 –** establishes and outlines function of Data Permit Authority to collect, combine, pre-process and disclose data for secondary use, as well as governance structures. Minister for Social affairs and Health appoints a steering committee every 3 years for the Data Permit Authority.[29]

Country	Data protection	Direct care	Beyond direct care	eHealth	Governance structures
New Zealand	**Privacy Act 2020** – provision for use of information for public health or public safety. Establishes principles for collection, use, disclosure of and access to information relating to individuals.[112] **Health Information Privacy Code 2020** – code of Practice issued by the Privacy Commissioner under section 32 of the Privacy Act which gives extra protection to health information because of its sensitivity.[21]	**Health Act 1956** – provisions in section 22 governing the disclosure of health information about identifiable individuals by and between health service providers and other agencies with statutory functions.[113] **Public Health and Disability Act 2000** – to facilitate access to, and the dissemination of information to deliver, appropriate, effective, and timely services -Section 3(1)(d).[121]	**Health Information Privacy Code 2020** – Health information obtained for one purpose may not be used for any other purpose, exceptions apply for example where individual is not identified, public health or public safety, research (for which approval by an ethics committee) and will not be published in identifiable form. [21] **Public Health and Disability Act 2000** – use and sharing of information for public health services and programmes.[121]	*No specific legislation for digital health services.*	**Privacy Act 2020 -** established the role of Privacy Commissioner to investigate complaints about interferences with individual privacy.[112] **Public Health and Disability Act 2000** – established the Health and Disability Ethics Committees (HDECs).[121]
Northern Ireland	**UK Data Protection Act 2018 –** (as outlined for England). [72][24] **ICO data sharing code of practice –** (as outlined for England).[72]	**Health and Social Care (Data Processing) Act (Northern Ireland), 2016 –** use of identifiable health information for health care or social care purposes which are in the public interest, without consent of individuals whose information may be used.[26] **Code of Practice on Protecting the Confidentiality of Service User Information, 2019 –** use and disclosure of personal identifiable information for the direct care of that service user.[28] **UK Data Protection Act 2018 –** (as above) [24]	**Data Protection Act 2018 –** (as above).[24] **Code of Practice on Protecting the Confidentiality of Service User Information, 2019 –** use and disclosure of personal identifiable information for purposes of health and social care not directly related to care of that service user (secondary uses) requires expressed consent or use of anonymised or pseudonymised data.[28]	*No specific legislation for digital health services.*	**Data Protection Act 2018 –** UK Information Commissioner (as above).[24] **Health and Social Care (Data Processing) Act (Northern Ireland), 2016 –** Department of Health to prepare and publish a code of practice on the processing of information.[26] **Code of Practice on Protecting the Confidentiality of Service User Information, 2019 –** Privacy Advisory Committee supports Personal Data Guardians and the Regional Quality Improvement Authority in ensuring that the information governance standards are maintained. [28]
Ontario (Canada)	**Privacy Act 1985** – to protect the privacy of individuals (public).[122] **PIPEDA 2000** – privacy law for private-sector organizations.[123] **Freedom of Information and Protection of Privacy Act and the Municipal Freedom of Information and Protection of Privacy Act, 1990** – to protect the privacy of individuals with information held by institutions.[124]	**The People's Health Care Act, 2019 –** outlines general rules on the use and sharing of personal health information.[125] **Personal Health Information Privacy Act (PHIPA), 2004 –** health information custodian may disclose personal health information about an individual, (a) to a health information custodian if the disclosure is reasonably necessary for the provision of health care and it is not reasonably possible to obtain the individual's consent in a timely manner, but not if the individual has expressly instructed the custodian not to make the disclosure.[27]	**Personal Health Information Privacy Act (PHIPA), 2004 –** a health information custodian may disclose personal health information about an individual, for audit or accreditation, improving provision of healthcare and improving quality of care, health protection or promotion or research if a research plan/application is approved.[27]	**Personal Health Information Privacy Act (PHIPA), 2004 –** Part v.1 Electronic Health Record**:** the prescribed organization has the power and the duty to develop and maintain the electronic health record in accordance with this legislation.[27]	**Privacy Act 1985 –** establishes the office and function of Privacy Commissioner of Canada.[122] **Personal Health Information Privacy Act (PHIPA), 2004 –** complaints, review and inspections responsibility of the Information and Privacy Commissioner in Ontario.[27]

Appendix 5: Summary of eHealth initiatives

Country	National health identifier	Electronic Health Records	ePrescribing	eReferral	Patient portal	Other
Australia	✓ Individual Healthcare Identifier	✓ My Health Record	✓ Electronic Pharmaceutical Benefits Scheme (PBS) prescription	✓ e-Referral	✓ Patient portal	
Denmark	✓ Unique patient identifiers	✓ Patients electronic record	✓ Shared Medication Record (Fælles Medicinkort FMK)	✓ eReferral	✓ Patient portal - Sundhed.dk	
England	✓ NHS number	✓ Local Health and Care Record Exemplar (LHCRE) – not universal	✓ Electronic Prescription Service (EPS)	✓ e-Referral Service (e-RS)	×	✓ Summary Care Records (SCRs)
Estonia	✓ Personal Identification Code	✓ National Health Information System (EHNIS)	✓ ePrescription	✓ eReferral	✓ Patient portal	✓ eAmbulance ✓ eConsultation ✓ X-Road (links private and public databases)
Finland	✓ Personal identity codes	✓ Electronic Health Records ✓ Patient Data Repository	✓ ePrescription	✓ eReferral	✓ Patient portal -My Kanta Pages	
New Zealand	✓ National health index	× National Health Information Platform- plans underway	✓ ePrescription Service (NZePS)	×	✓ Service Provided by GPs – not linked to EHR	✓ Shared Electronic Health Record
Northern Ireland	✓ Health and Care number (H&C number)	×	✓ Electronic Prescribing and Eligibility System (EPES)	×	✓ Patient portal (currently regional roll-out only with plans for national roll-out)	✓ Key Information Summary Record ✓ Northern Ireland Electronic Care Record (NIECR)
Ontario (Canada)	✓ Health number	✓ eHealth Ontario	✓ PrescribeIT – **not fully deployed**	✓ Ocean eReferral Network	×	

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