Health Information and Quality Authority

An tÚdarás Um Fhaisnéis agus Cáilíocht Sláinte

Health Information and Standards

International review of consent models for the collection, use and sharing of health information

February 2020

About the Health Information and Quality Authority

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

HIQA's mandate to date extends across a wide range of public, private and voluntary sector services. Reporting to the Minister for Health and engaging with the Minister for Children and Youth Affairs, 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, timely, relevant 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 Ireland's health and social care sector is highly fragmented, with major gaps and silos of information which prevent the safe, effective, transfer of information. This results in people using services being asked to provide the same information on multiple occasions.

In Ireland, information can also be lost, documentation is poor, and there is over-reliance 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.

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

Through its health information function, HIQA is working to support health and social care organisations in improving the quality of their data to better support the delivery, planning and monitoring of health and social care 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 information and the use and sharing of such information to improve care. Advances in digital technologies have the potential to improve the quality of care provided to patients and also promote organisational efficiency. However, it is important to ensure that individuals are fully informed about the use of their data and that they have a good understanding of how, and by whom, it will be used. Every individual should feel confident that their personal data and information will be used and protected appropriately.

In order to provide safe and effective care to the individual, health professionals should have the necessary patient data available to them. Individuals expect healthcare professionals and organisations to communicate effectively with each other in order to provide a high standard of care.[2] However, this is not always the case. Patients are often required to repeatedly relay their medical history to professionals, who may not have access to the patient's medical records. This leads to much duplication of efforts and can lead to suboptimal delivery of care.

The use of patient data for purposes beyond the delivery of care to the individual is also very important. This is often called 'secondary use of information'. The secondary use of information supports health and social care planning and management, the evaluation and improvement of services, policy development and research.

1.1 Purpose and scope of this background paper

The purpose of this background paper is to review national and international evidence and best practice in relation to models for the collection, use and sharing of personal health information. As this is a broad topic, this paper will focus on a number of key themes, specifically:

- eHealth initiatives
- legislation
- consent models
- public engagement
- information governance.

This background document will inform the development of recommendations on a model for the collection, use and sharing of personal health information in Ireland.

1.2 What is health information?

Health information is information extracted from patient records that can be used for a wide variety of purposes. Examples of this information include details of medical conditions, notes recorded by healthcare professionals and personal details such as date of birth. The term health information could refer to the whole record or just a part of it.

A list of key definitions relating to health information and how it is used can be found in Appendix 1.

1.3 How is health information used?

Health information can be used to provide direct individual care, and it can also be used for other purposes such as service planning and research.

The term 'individual care' describes the use of a person's health information for their own diagnosis, care and treatment by health and social care professionals. This is also known as primary use of health information or the use of information for direct care.

The term 'secondary use of information' describes the use of a person's health information for purposes beyond their own diagnosis, care and treatment. The two main types of secondary use are:

- service planning
- research.

In order to protect the privacy of the individual, health information can be changed to make it difficult or impossible to identify the individual about whom the data was collected. Health information can be personally identifiable, de-personalised or anonymous.

1.4 How is consent defined in the context of the collection, use and sharing of health information?

The General Data Protection Regulation (GDPR) provides the following definition of consent[3]:

'Consent' of the data subject means 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.

The traditional models of consent are opt-in (explicit consent) and opt-out (implied consent):

- Explicit consent/opt-in — an individual actively agrees or signs up to allow for data to be collected or used.
- Implied consent/opt-out — consent can be reasonably inferred and data will be collected and used automatically unless an individual actively dissents.

A list of key definitions relating to consent can be found in Appendix 2.

1.5 Methodology

The focus of this background paper is to determine current practices internationally in relation to the collection, use and sharing of personal health information with a focus on eHealth initiatives, legislation, consent, public engagement and information governance. In line with HIQAs recommendations development process; HIQA undertook a detailed desktop review to identify examples of best practice internationally. Experts in several regions were contacted for interview to ensure the most up to date information was gathered. The regions reviewed included:

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

An overview of the international evidence is provided in Chapter 3 and more detailed information on the consent model of each region is provided in Chapters 4 to 11.

2. Summary of current situation in Ireland

2.1 eHealth initiatives

Ireland's health system is currently predominantly paper based. However, there are plans to introduce eHealth initiatives such as an individual health identifier, ePrescribing, summary care records, shared care records and electronic health records. Some progress has been made in relation to the individual health identifier; the Health Identifiers Act was passed in 2014 and the Health Identifier Office was set up in 2019. The National Electronic Referral Programme was first piloted in 2011 and has continued to grow. General Practitioners across the country can now refer patients into every acute hospital electronically.

The eHealth Strategy of 2013 established eHealth Ireland, which has responsibility for overall governance around eHealth implementation including funding, legal enabling, public awareness, stakeholder engagement and building the 'eHealth Ecosystem'.[4] The Knowledge and Information Plan provides a roadmap for the delivery of the eHealth Strategy.[5]

The *Sláintecare Implementation Strategy* details clear plans to improve eHealth, and the *National Development Plan 2018–2027* expresses support for the provision of digital health services, including the development of electronic health records in healthcare settings such as the new Children's Hospital.[6,7]

A list of key definitions relating to eHealth can be found in Appendix 3.

2.2 Legislation

2.2.1 Data Protection Acts 1988–2018

These Acts govern the collection and processing of personal data. The Data Protection Act was adopted in 1988. It was amended in 2003 to transpose Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.[8] It was amended again in 2018 to give effect to the EU General Data Protection Regulation 2018 (GDPR, 2016/679). It established a new Data Protection Commission as the data protection authority with the means to supervise and enforce the protection standards enshrined in the regulation and directive. The Act also transposes the Law Enforcement Directive (Directive 2016/680/EU) into national law.[9]

The Department of Health introduced Health Research Regulations in 2018. They also intend to develop two further sets of regulations on the use of health information for individual care and for service planning.

The suitable and specific measures for data processing provided for in Section 36 of the Data Protection Act 2018 are given further and more specific effect through the Health Research Regulations 2018.

2.2.2 The Health Research Regulations 2018

The Health Research Regulations[10]:

- outline the mandatory suitable and specific measures for the processing of personal data for the purposes of health research
- provide a definition of health research for the purposes of the regulation
- provide for the possibility of applying for a consent declaration for new research
- provide for transitional arrangements in respect of the granting of consent declarations for health research that is already underway
- provide for the establishment and operation of a committee of persons to make decisions on applications for consent declarations, including an appeals process (the Health Research Consent Declaration Committee (HRCDC) was established in 2019)
- include a number of miscellaneous provisions.

2.2.3 The General Data Protection Regulation 2018 (GDPR)

A European Union-wide framework known as the General Data Protection Regulation (GDPR) came into force across the EU on 25 May 2018. An accompanying Directive establishes data protection standards in the area of criminal offences and penalties. This is known as the Law Enforcement Directive. The GDPR and the Law Enforcement Directive provide for significant reforms to current data protection rules. They provide for higher standards of data protection for individuals and impose increased obligations on organisations that process personal data. They also increase the range of possible sanctions for infringements of these rules.[3]

Under GDPR Personal data must be[11]:

- processed lawfully, fairly and in a transparent manner in relation to the data subject
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed
- accurate and kept up to date and every reasonable step must be taken to ensure that personal data that is inaccurate is erased or rectified without delay
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed

- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Article 9 of GDPR specifically deals with the processing of special categories of personal data, including data concerning health. Data concerning health can be processed if one of the following applies[10]:

- 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 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.

2.2.4 The Health Identifiers Act 2014

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. Section 11 of the Act permits health service providers and other entities, including the Health Research Board (HRB) and the National Cancer Registry Ireland (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 a secondary purpose. Authorised disclosees include the Central Statistics Office and health profession regulatory bodies. The definition of secondary purposes in the 2014 Act is quite narrowly cast: it includes '(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'.[12]

2.2.5 The Health (Provision of Information) Act 1997

The Health (Provision of Information) Act 1997 provides a general exception to the Data Protection Acts rules by allowing 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

from any person information held by or in the possession of that person. That person may provide any personal information to the National Cancer Registry Board for the purpose of any of its functions or to the Minister for Health or any other body or agency for the purpose of compiling a list of people who may be invited to participate in a cancer screening programme authorised by the Minister. Under the amendment to the Health (Provision of Information) Act 1997 by the Data Protection Act 2018, compliance with the request for the provision of information to the National Cancer Register is made mandatory.(13)

2.3 Consent model

Other than the Health Research Regulations 2018, there is no specific health information related legislation or regulations in Ireland that address consent with respect to the collection, use and sharing of personal health information. Consent to the processing of health data must be obtained unless one of the exceptions in the Data Protection Acts or GDPR applies. Exceptions may allow processing of special categories of personal data without the consent of the data subject for reasons of public interest, such as, for public health purposes.(14)

In relation to the secondary use of health information, the Health Research Regulations 2018 set out specific safeguards (as required under GDPR) which must be in place before personal data can be processed for health research, including requirements for explicit consent and prior approval by a research ethics committee. Where the requirement to obtain consent cannot be met, data controllers may apply to the Health Research Consent Declaration Committee for a declaration that explicit consent is not needed as the public interest in carrying out the research concerned significantly outweighs the need for consent.(10)

The Department of Health intend to develop two further sets of Regulations on the use of health information for individual care and for service planning.

2.4 The role of the Data Protection Commission

The Data Protection Commission (DPC) is the national independent authority in Ireland responsible for upholding the fundamental right of individuals in the European Union (EU) to have their personal data protected. Accordingly, the Data Protection Commission is the Irish supervisory authority responsible for monitoring the application of the General Data Protection Regulation (GDPR). The statutory powers, duties and functions of the DPC are as established under the Data Protection Act 2018, which gives further effect to the GDPR, and also gives effect to the Law Enforcement Directive.(9)

Using its statutory powers, the Data Protection Commission[15]:

- examines complaints from individuals in relation to potential infringements of data protection law
- conducts inquiries and investigations regarding infringements of data protection legislation and takes enforcement action where necessary
- promote awareness amongst members of the public of their rights to have their personal information protected under data protection law
- drives improved awareness and compliance with data protection legislation through the publication of high-quality guidance, proactive engagement with public and private sector organisations
- assists in identifying risks to personal data protection and offers guidance of best practice methods to mitigate against those risks
- cooperates with (which includes sharing information with) other data protection authorities, and acts as Lead Supervisory Authority at EU level for organisations that have their main EU establishment in Ireland.

2.5 Patient and public attitudes to the collection, use and sharing of personal health information

A systematic review on public views on the use of patient data in Ireland and the UK found the following[16]:

- There is a general willingness to share patient electronic health records for 'secondary purposes like research, policy and planning' as it is associated with 'the greater good'.
- In relation to privacy, control is very important to individuals. Individuals want to feel in control of how their information is accessed and used.
- Public trust depends on the organisation's ability to guarantee privacy and security and also on the organisation's motivations.

In summary, there is general support for the use of personal health information to benefit society through secondary use. However, the public needs to be aware how this information will be stored and processed.

3. Summary of international evidence

This background paper focuses on consent, legislation, eHealth initiatives and public engagement in eight different regions. In line with HIQA's recommendations development process, HIQA undertook a detailed desktop review to identify examples of best practice internationally. Experts in several regions were contacted for interview to ensure the most up to date information was gathered. The regions reviewed were England, Northern Ireland, New Zealand, Australia, Estonia, Canada, Finland, Denmark. The information garnered from this review will inform the recommendations HIQA make for the collection, use and sharing of health information in Ireland.

Implied consent is used in each of the regions for the provision of care to the individual. All regions reviewed allow anonymised health information to be used for service planning and research purposes. Consent is generally needed in order to use identifiable health information for secondary purposes.

Most regions use ethics boards to grant access to identifiable health information for research. A key finding from this review was that in order to successfully implement a consent model, it is necessary to consult and engage with the public. The public should be able to trust that their personal health information is safe and used appropriately in ways that are acceptable to them. Public engagement is essential in order to learn what is acceptable to people and what level of trust currently exists. Engagement must be ongoing in order to build and maintain public trust. It is also important to educate the public on the benefits of information sharing across the health system.

In 2013, England tried to implement a national database of patient interactions with the healthcare system called care.data. Following three years of debate and controversy, the care.data scheme was closed in 2016. England has made substantial efforts in engaging with the public since the failings of the care.data initiative. The Understanding Patient Data organisation was set up to support better conversations about the uses of health information between healthcare providers, government and the public. This has helped England rebuild trust by emphasising the need and requirement to keep the public informed about how their personal health information is used. New Zealand and Canada also have good examples of effective public engagement such as the Data Futures Partnership Our Data, Our Way and Canada Health Infoway's Canada's Better Health Together workshop.

Ireland has the advantage of learning from other countries that have a more mature eHealth infrastructure, such as those included in this review.

Countries such as Estonia, Finland and Denmark have a culture of trust and openness. The culture of trust and openness is built on public engagement, strong

data security infrastructure (such as the use of blockchain technology), the use of legislation to protect service user's health information and the ease of access to personal health information. From this international review, it is evident that public trust, transparency around how data will be used and information security are key enablers to successful implementation of eHealth initiatives.

Legislation is in place in each of the regions that governs where identifiable health information can be used without consent, for example, for public health purposes. Where legislation exists for the secondary use of health information, clear rules are established about how and when identifiable health information can be used. This creates a culture of trust between patients and healthcare providers because patients know their personal health information is protected and also means that their data can be used in a secure way for health research and service planning activities. Having clear legislation/codes of practice on how health information can be collected, used and shared is mutually beneficial for health service providers, healthcare professionals, researchers, patients and the public.

All of the regions have data protection legislation in place, and the European countries are all governed by the General Data Protection Legislation (GDPR). Some regions have introduced health information specific legislation. Examples include:

- Ontario's health privacy legislation, the Personal Health Information Protection Act (PHIPA), which establishes a set of rules regarding personal health information (PHI).[17]
- Finland's Act on the Handling Customer Data in Health and Social Care, which aims to strengthen the data security of processing patient information and patients' access to information.[18]

Some of the regions have developed codes of practice that govern the consent model that is in place. These include:

- Northern Ireland's *Code of Practice on Protecting the Confidentiality of Service User Information*. The code of practice provides support and guidance for all those involved in health and social care regarding decisions about the protection, use and disclosure of service user information.[19]
- New Zealand's *Health Information Privacy Code*. The code sets out particular rules for agencies in the health sector on the collection, use, storage and disclosure of health information by health agencies.[20]

Some of the regions have introduced specific legislation or frameworks in relation to the secondary use of health information.

- Finland has introduced an act specifically in relation to the secondary use of health data. The Act on Secondary Use of Health and Social Data 2019 has been introduced to facilitate the effective and safe processing and access to

the personal social and health data for steering, supervision, research, statistics and development in the health and social sector.[21]

- Australia has developed a *Framework to guide the secondary use of My Health Record system data* that describes the governance mechanisms and technical processes to be implemented before data can be released for research, policy and planning secondary purposes.[22]

4. England

It is estimated that the population of England is over 55 million.[23] Healthcare in England is mainly provided by England's public health service, the National Health Service (NHS).[24]

eHealth at a glance:

- national health identifier — NHS number
- Summary Care Records — 60 million in use, opt-out rate of 1.2%
- Local Health and Care Record Exemplars (LHCRE) — regional collaboration to develop integrated care records in specific regions
- ePrescribing — expected to reach 90% coverage by 2020
- NHS eReferral Service — in use by all general practitioners (GPs) and hospital trusts.

Consent model overview:

- Implied consent is used for the provision of individual care.
- A national data opt-out is in place to allow individuals to opt-out of having their confidential personal information used for secondary purposes such as service planning and research.
- The national data opt-out does not apply to anonymised data.
- Individuals can also opt-out of having a Summary Care Record.

3.1 Key organisations

There are a number of key organisations with varying responsibilities in relation to personal health data (collection, use and sharing) in England. These include:

- NHS England
- NHS Digital
- Public Health England
- The National Data Guardian
- NHSX
- The Information Commissioner's Office.

4.1.1 NHS England

Information has been described as the lifeblood of the NHS. As such, it is a vital asset for the clinical management of individual patients and the efficient management of services throughout the NHS. Within NHS England, the Chief Data

Officer's team is responsible for the development and delivery of a strategy for the use of data at every level of the organisation.(25)

The health sector handles some of the most sensitive personal data, and patients have the right to expect that information will be looked after. The Secondary Uses Service (SUS) is the single, comprehensive repository for healthcare data in England that can be used for a range of reporting and analyses to support the NHS in the delivery of healthcare services. SUS is a secure data warehouse that stores this patient-level information in line with national standards. Access to SUS is managed using role-based access control (RBAC), which grants appropriate access levels to identifiable, anonymised or pseudonymised data based on the users job role.(26)

4.1.2 NHS Digital

NHS Digital has responsibility for standardising, collecting and publishing data and information from across the health and social care system in England. Within NHS Digital, the Information Governance Alliance (IGA) is the authoritative source of advice and guidance about the rules on using and sharing information in healthcare. The core members of the Information Governance Alliance are the Department of Health, NHS England, NHS Digital and Public Health England. Representatives from the Information Commissioner's Office and the National Data Guardian's Office also sit on the Board.(26)

NHS Digital Spine supports the IT infrastructure for health and social care in England, joining together over 23,000 healthcare IT systems in 20,500 organisations. Spine allows information to be shared securely through national services such as the Electronic Prescription Service, Summary Care Records and the e-Referral Service.(27)

4.1.3 Public Health England

Public Health England is an executive agency of the Department of Health and Social Care and a distinct organisation with operational autonomy. It collects and publishes statistics on public health topics, including health protection and health improvement. It is responsible for researching, collecting and analysing data to improve our understanding of public health challenges and to come up with answers to public health problems.(28)

4.1.4 National Data Guardian

The National Data Guardian (NDG) role was created in November 2014 to be an independent champion for patients and the public on confidential health and care information. The purpose of the role is to make sure that people's information is kept safe and confidential and that it is shared when appropriate to achieve better outcomes for patients. The NDG does so by offering advice, guidance and encouragement to the health and care system. In December 2018, the Health and Social Care (National Data Guardian) Act 2018(29) placed the NDG role on a statutory

footing and granted it the power to issue official guidance about the processing of health and adult social care data in England.[30] Key guidance in relation to the collection use and sharing of health information includes:

- the Information Governance Review, 2013[2]
- the Review of Data Security, Consent and Opt-outs, 2016.[31]

4.1.5 NHSX

NHSX brings teams from the Department of Health and Social Care, NHS England and NHS Improvement together into one unit to drive digital transformation and lead policy, implementation and change. NHSX aim to deliver the *'the future of healthcare: our vision for digital, data and technology in health and care'* building on the *NHS Long Term Plan*. NHSX has set five missions[32,33,34]:

- reducing the burden on clinicians and staff, so they can focus on patients
- giving people the tools to access information and services directly
- ensuring clinical information can be safely accessed, wherever it is needed
- improving patient safety across the NHS
- improving NHS productivity with digital technology.

NHSX has responsibilities around[32]:

- coordination and consistency
- setting standards
- driving implementation
- radical innovation
- common technologies and services
- reforming procurement
- cyber policy
- digital capability
- governance.

4.1.6 Information Commissioner's Office

The Information Commissioner's Office (ICO) is the UK's independent body set up to uphold information rights and the UK's data protection regulator. As part of their role in supporting the sector, the ICO's good practice team carries out audits and advisory visits across a broad range of health organisations. They provide practical tools that data protection officers, records managers and information governance specialists can use to help educate colleagues on how to ensure they are operating in line with the Data Protection Act. Examples of tools and guidance they provide include:

- guidance on consent[35]
- *Code of practice on confidential information*[36]

- *Anonymisation: managing data protection risk code of practice.*[37]

4.2 Legislation

Important legislation in place in England in relation to the collection, use and sharing of personal health information includes:

- The Health and Social Care (Safety and Quality) Act 2015
- Health Service (Control of Patient Information) Regulations 2002
- Access to Health Records Act 1990 (England, Scotland and Wales)
- Access to Medical Reports Act 1988 (England, Scotland and Wales)
- Data Protection Law
- The NHS Constitution.

Legislation	Description
The Health and Social Care (Safety and Quality) Act 2015	The Health and Social Care (Safety and Quality) Act 2015 places a duty on health and adult social care providers to share information about a person's care with other health and care professionals.[38] All health and adult social care organisations must, by law, share information with each other about patients they are caring for directly, to improve the care provided. They must also use a patient's NHS number as a consistent identifier when sharing data or information about them.[39]
Health Service (Control of Patient Information) Regulations 2002	The Health Service (Control of Patient Information) Regulations 2002 establish a legal basis in England and Wales for data to be disclosed for public health purposes without patient consent. Under the Regulations, there is more than one potential route towards lawful processing: Data may be processed for public health purposes under both Regulations 3 and 5.[40]
Access to Health Records Act 1990 (England, Scotland and Wales)	This legislation provides rights of access to a deceased patient's personal representative and any person who may have a claim arising out of a patient's death. Where an application is made by a person who may have a claim, access to patient records is limited to information of relevance to the claim.[41]

Access to Medical Reports Act 1988 (England, Scotland and Wales)	This legislation gives patients the right to see medical reports written about them for employment or insurance purposes, by a doctor who is or has been responsible for the patient's clinical care. Patients have the right to ask the doctor to amend any part of the report that the patient considers to be incorrect or misleading. They also have the right to record their disagreement to the contents of the report in a statement attached to the report or withdraw their consent for the release of the information.[42]
Data Protection Law	The Data Protection Law, including the Data Protection Act 2018[43] and GDPR,[44] focuses on doctors ethical and legal duties of confidentiality. However, the processing of personal data must also satisfy the requirements of Data Protection Law, which imposes different duties on data protection. The law allows personal data to be shared between those offering care directly to patients but it protects patients' confidentiality when data about them are used for other purposes. These secondary uses of data are essential in order to run a safe, efficient and equitable health service. They include[43]: – reviewing and improving the quality of care provided – researching what treatments work best – commissioning clinical services – planning public health services.
The NHS Constitution	The NHS Constitution makes it clear that everyone has the right to be informed about how their information is used and the right to request that their confidential information is not used beyond their own care and treatment. Where their wishes cannot be followed, they should be told the reasons, including the legal basis. The NHS Constitution also lays out clearly that the NHS will anonymise information contained in medical records for use by researchers to support healthcare improvement.[45]

4.3 Consent model

4.3.1 Individual care

Explicit consent is not required for the purposes of providing care to the individual in England: this consent is implied as part of the provision of individual care. Individual care is described as[31]:

> A clinical social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals. It includes supporting individuals' ability to function and improve their participation in life and society.
>
> It includes the assurance of safe and high quality care and treatment through local audit the management of untoward or adverse incidents, person satisfaction including measurement of outcomes undertaken by one or more registered and regulated health or social care professionals and their team with whom the individual has a legitimate relationship for their care.

The use of personal confidential data for local clinical audit is permissible within an organisation with the participation of a health and social care professional with a legitimate relationship to the patient through implied consent. For audit across organisations, the use of personal confidential data is permissible where there is approval under Regulation 5 of the Health Service (Control of Patient Information) Regulations 2002.[40]

4.3.2 Uses beyond the care of the individual

In June 2016, Dame Fiona Caldicott, the National Data Guardian in the UK, published *National Data Guardian for Health and Care – Review of Data Security, Consent and Opt-Outs*. In this review, she recommended a new consent/opt-out model which would give people a clear choice about how their personal confidential data is used for purposes beyond their direct care.[31]

In response to this, the Department of Health published *Your Data: Better Security, Better Choice, Better Care.*[46] This document sets out the plan to implement the recommendations made by the National Data Guardian.[46]

A national opt-out has been implemented that allows patients to opt-out of their confidential patient information being used for research and planning. It was introduced in May 2018. An online service is available to all patients where they can view or change their opt-out choice at any time. By 2020, it will be mandatory for all health and social care organisations to be compliant with the national opt-out policy. NHS Digital and Public Health England are already compliant.[47]

In order to achieve this goal, the Department of Health have committed to[46]:

- support professionals in implementing the national opt-out
- support legislation to put the role of the National Data Guardian on a statutory footing
- implement stronger measures to protect personal data
- work with stakeholders to develop communication tools to explain the opt-out to the public
- ensure that patients can access and understand how their data has been used nationally by 2020.

As of March 2019, the opt-out rate was 2.74% of registered patients.[48] Some specific rules relating to the national opt out include the following[49].

- The opt-out applies regardless of the format of the data and this includes structured and unstructured electronic and paper records.
- When the opt-out is applied, the entire record (or records) associated with that individual must be fully removed from the data being disclosed.
- The opt-out does not apply to information that is anonymised in line with the ICO's *Code of Practice on Anonymisation* or is aggregate or count type data.
- The opt-out is defined based on purpose and applies to any disclosure of data for purposes beyond individual care.
- A person may give consent for a specific purpose, such as a research project, either before or after setting a national data opt-out and this consent will constitute an exemption from the national data opt-out.
- The opt-out continues to be maintained and applied for an individual after they have died.
- Individuals aged over 13 are able to set a national opt-out. Those with parental responsibility are able to set a national opt-out on behalf of a child under the age of 13 via the non-digital channel only.

There are some circumstances where the national data opt-out does not apply, these include[49]:

- the monitoring and control of communicable disease and other risks to public health.
- where there is an overriding public interest in the disclosure
- where the information is required by law or a court order
- where data is used for payment and invoice validation purposes
- for the purpose of allowing participation in national screening programmes
- information about people with learning disabilities and/or autism who are in hospital for their mental health or due to challenging behaviour
- the National Cancer Patient Experience Survey and Care Quality Commission's NHS Patient Survey Programme

- open data or statistics published by NHS Digital where this is subject to disclosure controls and is fit for publication.

4.4 eHealth developments

There are a number of eHealth initiatives in use in England, including:

- the national health identifier (NHS number)
- Summary Care Records
- Local Health and Care Record Exemplars
- Electronic Prescription Service (ePrescribing)
- NHS eReferral Service.

4.4.1 National health identifier

An NHS number is given to every citizen registered with the NHS in England, Wales and the Isle of Man (the Community Health Index (CHI) is used in Scotland). It is given to the patient when they register with a GP practice, and it allows for healthcare staff to match details to health records.[50,51,52] There is no option to opt-out of this but if you have requested the national data opt-out, your personal data will not be used for purposes beyond your individual care.

4.4.2 Summary Care Records

Summary Care Records (SCRs) are an electronic record of important patient information, created from GP medical records. Generally access to SCR information means that care in other settings is safer, reducing the risk of prescribing errors. It also helps avoid delays to urgent care. At a minimum, the core SCR holds important information about:

- current medication
- allergies and details of any previous bad reactions to medicines
- the name, address, date of birth and NHS number of the patient.

SRCs can be seen and used by authorised staff in other areas of the health and care system involved in the patient's direct care. The SCR was set up in 2007, and, while the uptake was slow at the time, the majority of people in England have an SCR. There are approximately 60 million SCRs in use and there is an opt-out rate of 1.2%, which equates to 3.1 million people. The SCR is currently used for individual care only and not used for secondary purposes beyond the care of the individual.[53]

The patient can also choose to include additional information in the SCR. When a patient consents to including additional information in their SCR, the GP can add it simply by changing the consent status on the clinical system. This means more information will be available to health and care staff viewing the SCR. Additional information may include[54]:

- significant medical history
- reason for medication
- anticipatory care information (such as information about the management of long term conditions)
- end-of-life care information
- immunisations.

The patient is asked at the GP practice whether they would like to set up a summary care record. If the patient says no, then a summary care record is not set up and, thus, a SCR for this patient cannot be accessed, even in an emergency, as it does not exist. The following controls are in place in relation to SCRs to ensure access is in line with the Care Record Guarantee[55]:

- authentication and role-based access control (RBAC) — use of smartcards
- legitimate relationships (LR) — the viewer has a good reason to view the patient's SCR as they are involved in their care
- permission to view (PTV) — the patient is asked for their consent before the SCR is viewed. Emergency access is allowed if it is in the patient's best interest, for example, if they are unconscious or cannot communicate. Permission to view can be gained each time or it can cover future use as long as the question asked makes this clear to the patient and there is a clear system for recording this.

Legitimate relationships and permission to view (or emergency access, with explanation noted) can be recorded by a member of staff, such as a receptionist or by the clinician themselves. When a healthcare professional self-claims a legitimate relationship or when they use emergency access, an alert will be generated. These alerts will be audited by each organisation's privacy officer to make sure there was a valid reason for the view.[55]

Every organisation that views SCRs must appoint a privacy officer. The privacy officer has codes added to their smartcard so that they can access the Alert Viewer on the Spine and check whether SCR views were legitimate. For alerts where the clinician has self-claimed a legitimate relationship, the privacy officer will confirm that the patient was being treated at the organisation by looking at the Patient Administration System or another record of patient attendance.[55]

The national data opt-out applies to the SCR; however, the data is not currently used for secondary purposes.

4.4.3 Local Health and Care Record Exemplars

A Local Health and Care Record Exemplar (LHCRE) is a regional collaboration across health, care and local authorities to develop shared health records for the people in the region. The LHCRE were launched in 2018. Their aim is to design shared

records for improving and coordinating individual care. The intention is that, regardless of where an individual is receiving care and support (at their GP, hospital, community hospital or even at home), the health professionals looking after them can access the right information, at the right time.

There are already many LHCREs across England (for example the Dorset Care Record and Leeds Care Record); while creating better joined up care for hundreds of thousands of people, they are being designed and delivered independently of each other. The lack of common standards means there is a danger of developing new information silos that cannot support care when an individual moves between areas or when someone's needs might be best served at a wider geographical level, for example at a national centre for a rare disease.(56)

The primary focus of the LHCRE is to create integrated health and care records for individual care. However, NHS England's five regions are also considering how shared health and care records could be used to support purposes beyond individual care, such as improving health and services through research and planning.(56)

The models used to protect patient data vary among the LHCRE. Information on the model used by the Great North Care Record is given below(57):

- The Great North Care Record is viewed via a secure and encrypted system that meets NHS security standards.
- The system keeps a record of everyone who has accessed a patient record, the time and date when they accessed it and the information they were viewing.
- Regular checks are made to make sure that only people who need to see your patient record are viewing it.
- A patient will be asked for permission to view the record at the point of care, they will be given the option to opt-out at this stage.
- A patient can also choose to opt-out of having a care record. This can be done by returning a form to the GP or by phone.

4.4.4 ePrescribing

The NHS Electronic Prescription Service (EPS) allows GPs and other prescribers to send prescriptions electronically to a dispenser (such as a pharmacy) of the patient's choice. Eventually EPS will remove the need for most paper prescriptions. This makes the prescribing and dispensing process more efficient and convenient for patients and staff. EPS is now used in additional care settings, such as integrated urgent care.(58)

The fourth phase of the EPS pilot involved launching the system in four GP practice pilot sites in November 2018. In July 2019, EPS phase four was live in 56 GP

practices, with around 2,000 pharmacies having dispensed a phase four prescription. It is expected that by the end of 2020, the proportion of prescriptions issued through the electronic prescription service will be over 90% of all prescriptions.(59)

In order to use this service, patients are asked to nominate a pharmacy. Consent is required for this process. Patients can opt-out of using the system at any time and they can also choose to change the nominated pharmacy.(60)

4.4.5 NHS eReferral Service

The NHS e-Referral Service (e-RS) combines electronic booking with a choice of place, date and time for first hospital or clinic appointments. It was fully rolled out in 2018. Patients can choose their initial hospital or clinic appointment, which they can then book online (a telephone service is also available) or in the GP surgery at the point of referral. All 150 acute hospital trusts and GP practices have made the move to sending and receiving all first outpatient referrals through the NHS e-Referral Service.(61)

Consent is not required for the e-Referral service. This data is processed under GDPR using the lawful basis of legal obligation and management of health and social care systems.(62)

4.4.6 care.data

In 2013, NHS England set up care.data, a national database of patient interactions with the healthcare system. A leaflet was sent to 22 million homes which gave information on the project. However, it did not detail any of the benefits that the scheme would provide to the public and many households did not read the leaflet. The leaflet told people to contact their GP if they did not want their information shared. There was no other information on the opt-out process and it was widely believed that this process would place strain on the GP system. Without sufficient information on the scheme, people did not feel informed about NHS England's scheme and feared that the data might not be treated with the sensitivity that it deserved.(63)

Prior engagement with the public is seen as an area that NHS England failed with the care.data scheme. The care.data scheme was closed in 2016 after years of debate and controversy.

4.5 Patient engagement

4.5.1 Understanding Patient Data

Understanding Patient Data is an initiative that has been set up to support better conversations about the uses of health information. The aim of the initiative is to explain how and why data can be used for care and research, what is allowed and what is not, and how personal confidential information is kept safe. Understanding Patient Data aims to support discussions with the public, patients and healthcare professionals about uses of health and care data by[64]:

- providing objective evidence about:
  - how and why data can be used for care and research
  - the benefits and risks
  - what is allowed and not allowed
  - how personal information is safeguarded
- helping people make informed decisions when they have options about how data might be used
- developing advocates who can champion the responsible use of data
- bringing together, and partnering with, other engagement initiatives to strengthen the voice of individual activities
- working with the media to present an even-handed portrayal of stories relating to health data
- providing analysis about public attitudes to help inform NHS England, Department of Health and NHS Digital policy and communications
- examining emerging issues from new data-driven technologies and the implications for public confidence.

An evaluation of the impact of Understanding Patient Data was carried out in 2018 and concluded that Understanding Patient Data has[65]:

- achieved what it was set up to do — influencing both policy decisions and enabling better public engagement
- shone a light on the need to inform and engage with the public around the use of their data
- worked as a bridge between local conversations and national level policy and debate.

4.5.2 Understanding public expectations of the use of health and care data

A report was commissioned by the OneLondon LHCRE to help design and develop an approach to the sharing of patient health and care information. The report will inform engagement with the public to ensure that patient data is shared in a way that is in line with public expectations. The report collates and synthesises existing knowledge about public expectations and attitudes towards the sharing of patient

health information and gives an overview of the results of stakeholder interviews that were carried out during the review. Key findings include[66]:

- Most people expect their medical records to be available to the full range of NHS clinicians providing direct individual care.
- There is surprise that different health professionals in different places within the NHS are not already able to access health records.
- There are expectations that individuals should know exactly what information will be made available to users of shared data systems and will have the opportunity to exercise some control over which items should be shared, and with whom.
- There is relatively little published information on the actual views of those most in need of protection, such as vulnerable users of mental health services.
- There is much less evidence available on attitudes towards the use of patient data for service planning than there is for its use in research.
- Support for secondary uses of health information is higher when the information is de-personalised.
- Clarity in the intended use of patient data is very important to both professional staff and patient representatives.
- Many stakeholders could see significant potential benefits leading to genuine improvement in overall healthcare provision.
- There is good evidence for public support for sharing patient data for the purposes of medical research.

4.6 Key learnings

- England has a national health identifier, Summary Care Records, ePrescribing, eReferral and LHCREs in place.
- Implied consent is used for the provision of individual care.
- Consent is not required for the e-Referral Service. This data is processed under GDPR using the lawful basis of legal obligation and management of health and social care systems.
- A national data opt-out was introduced in 2018 and will be fully implemented by 2020. This allows patients to opt-out of their confidential patient data being used for research and planning. The opt-out does not apply to anonymised data.
- The NHS Constitution makes it clear that everyone has the right to be informed about how their information is used and the right to request that their confidential information is not used beyond their own care and treatment.
- Summary Care Records are set up by a GP practice if consent is given by the patient to do so. Individuals can opt-out of having a Summary Care Record. If the patient declines, a Summary Care Record will not be created for that patient.
- LHCRE have been set up as regional collaborations across health, care and local authorities to develop shared health and care records for the people in their region. The model used for the collections use and sharing of patient data varies between LHCRE.
- Prior engagement with the public is seen as an area that NHS England failed with the care.data scheme.
- Understanding Patient Data is an initiative that has been set up to support better conversations about the uses of health information. This initiative has enabled better engagement with the public on projects such as the national data opt-out.

5. Northern Ireland

In Northern Ireland, the health service is referred to as Health and Social Care (HSC). While the HSC is run separately from the British National Health Service (NHS), many of its features are shared. As with the NHS, is it free at the point of delivery. However, HSC also provides social care services such as home care services, family and children's services, day care services and social work services. The Department of Health has authority for health and social care services.[67]

eHealth at a glance:

- National health identifier — Health and Care Number
- Northern Ireland Electronic Care Record (NIECR) — launched in 2013
- ePrescribing — operational since 2008.

Consent model overview:

- Implied consent is used for the provision of individual/direct care. Service users must be informed of what information sharing is necessary for their care.
- Identifiable data can be used for uses beyond direct care if required by law or if explicit consent has been obtained.
- Explicit consent is required if identifiable data is used for research purposes. Anonymised data can be used without consent.
- The Northern Ireland Electronic Care Record (NIECR) has moved away from its original consent model (informed consent) and will now process data under the legal basis of 'public task' in order to comply with GDPR. Consent will no longer be required to process NIECR data.

5.1 Key organisations

There are a number of key organisations with varying responsibilities in relation to personal health data (collection, use and sharing) in Northern Ireland. These include:

- the Department of Health
- Health and Social Care (HSC)
- E-Health and Social Care
- the Information Commissioner's Office
- the Privacy Advisory Committee

5.1.1 The Department of Health

The Department of Health in Northern Ireland has three main business responsibilities[68]:

- Health and Social Care (HSC), which includes policy and legislation for hospitals, family practitioner services and community health and personal social services
- Public Health, which covers policy, legislation and administrative action to promote and protect the health and well-being of the population
- Public Safety, which covers policy and legislation for fire and rescue services.

5.1.2 Health and Social Care (HSC)

Health and Social Care in Northern Ireland is provided as an integrated service. There are a number of organisations who work together to plan, deliver and monitor Health and Social Care across Northern Ireland[67]:

- Health and Social Care Board (HSCB)
- Health and Social Care Trusts
- Public Health Agency (PHA)
- Patient and Client Council (PCC)
- the Business Services Organisation
- Regulation and Quality Improvement Authority (RQIA).

5.1.3 E-Health and Social Care

E-Health and Social Care is delivering a programme of improvement for health and social services in Northern Ireland. It is about supporting change in the way the HSC delivers its services to patients and service users for the better by making the best use of information and communication technologies. E-Health and Social Care is tasked with procuring, developing and implementing new integrated ICT infrastructure and systems for all HSC organisations, such as the secure HSC network and regional data centres. The programme is working towards three strategic goals[69]:

- Electronic care records containing the information and images generated from patient/client contacts
- Electronic care communications enabling fast, secure exchange of information between care professionals within and between the various HSC organisations
- Electronic information providing patients, service users and care professionals with details of best practice and up-to-date information for making decisions about diagnosis, treatment and the services available.

5.1.4 Information Commissioner's Office (ICO)

This office is the United Kingdom's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.[70] Further detail can be found in Section 4.1.6.

5.1.5 Privacy Advisory Committee

The Privacy Advisory Committee was established in 2006, and its principal role is to advise HSC bodies about the use of information relating to patients and clients. The Chairperson is appointed by the Department of Health and the members are drawn from a wide range of individuals, including health and care professionals and service users. The Privacy Advisory Committee has the following ongoing responsibilities[71]:

- To oversee the implementation of the recommendations agreed by the Minister on protecting personal information.
- To manage a project team to complete a programme of work to give effect to the recommendations agreed by the Minister.
- To report regularly to the Department on progress on implementing the recommendations.
- To keep consent and confidentiality matters in Health and Personal Social Services (HPSS) under continuous review and to provide timely and relevant best practice advice to HPSS bodies.
- To consider current and new uses to which personal information is put in HPSS bodies and to authorise such uses of personal information taking particular account of the legal and ethical issues surrounding privacy and confidentiality.

5.2 Legislation

Important legislation in place in Northern Ireland in relation to the collection, use and sharing of personal health information includes:

- The Data Protection Act 2018
- Freedom of Information Act 2000
- The Privacy and Electronic Communications Regulations 2003
- Health and Social Care (Data Processing) Act (Northern Ireland) 2016
- Code of Practice on Protecting the Confidentiality of Service User Information

Legislation	Description
The Data Protection Act 2018	The Data Protection Act gives an individual freedom of information and data protection. It gives a person the right ask any public sector organisation for the information they hold in general or about them. Some sensitive information might not be available to members of the public. If this is the case and a person's request is denied, they have the right to ask why it is upheld. If they do not get a sufficient reason for this, they can make a complaint to the Information Commissioner's Office. General Data Protection Regulation (GDPR) control how a person's personal information is being used by organisations. Everyone who collects data has to follow rules called data protection principles. Data protection principles ensure:(72) ▪ information is processed in a transparent way ▪ collected for legitimate purposes ▪ accurate and up to date ▪ kept for no longer than necessary ▪ processed in a safe and secure way. Under data protection legislation, a person has the right to be informed, access information, right to rectification, erasure, restrict processing, data portability and to object.(73)
Freedom of Information Act 2000	The Freedom of Information Act 2000 gives members of the public a general right of access to recorded information held by public authorities. It also requires public authorities to adopt and maintain a publication scheme.(74)
The Privacy and Electronic Communications Regulations 2003	The Privacy and Electronic Communications Regulations (PECR) sit alongside the Data Protection Act and the GDPR. They give people specific privacy rights in relation to electronic communications. These are marketing calls, emails, texts and faxes, cookies (and similar technologies), keeping communications services secure and customer privacy as

	regards traffic and location data, itemised billing, line identification, and directory listings.(75)
Health and Social Care (Data Processing) Act (Northern Ireland) 2016	The policy provides a clear statutory framework and robust and stringiest safeguards which will enable use of health and social care information which identifies individuals to be used for health or social care purposes without the consent of individuals whose information may be used. The provisions of the act will only be used when it is impossible to receive anonymous data. There are six sections to the act:(76) ▪ control of information ▪ establishment of a committee to authorise processing of health information and the dissemination of information ▪ code of practice ▪ regulations ▪ interpretation of definitions of specific terms within the act ▪ short title and commencement dates.

5.2.1 Code of Practice on Protecting the Confidentiality of Service User Information

The Code of Practice on Protecting the Confidentiality of Service User Information provides support and guidance for all those involved in health and social care, concerning decisions about the protection, use and disclosure of service user information. The code was developed by the Privacy Advisory Committee following a comprehensive round of public consultation in 2011. The code was updated in 2019 to take account of GDPR. Healthcare professionals are required to pay due regards to the Code of Practice under the Health and Social Care (Data Processing) Act (Northern Ireland) 2016.(19)

This Code of Practice is principally concerned with identifiable service user information. Uses or disclosures of such information are only justified in any of the following situations(19):

- the service user has given his or her consent
- there is a statutory requirement to use or disclose the information
- the balance of public and private interests favours disclosure. In such situations, there must be a substantial public interest favouring disclosure

which outweighs both the private interests of the individual and the public interest in safeguarding confidentiality.

The nature of the obligation to protect confidentiality can be expressed in terms of three core principles[19]:

- individuals have a fundamental right to the confidentiality and privacy of information related to their health and social care
- individuals have a right to control access to and disclosure of their own health and social care information by giving, withholding or withdrawing consent
- when considering whether to disclose confidential information, health and social care staff should have regard to whether the disclosure is necessary, proportionate and accompanied by any undue risks.

5.3 Consent model

5.3.1 Individual care

In Northern Ireland, the definition of direct care includes clinical audit and case review carried out by members of the care team and those supporting them, for the purpose of improving the direct care of that service user.

The Code of Practice on Protecting the Confidentiality of Service User Information states the following[19]:

- 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.
- 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.
- Review of care carried out by members of the care team and those supporting them have sufficient connection with that direct care for the sharing of information to be justified on the basis of implied consent, provided the individual has been informed.
- Where it is planned to involve staff from other agencies this should first be discussed with the service user and their explicit consent sought.
- When other agencies request information about service users, health and social care staff should seek the consent of the service user.
- In situations of on-going need for care and support, the potential benefits of information sharing with their informal carers should be discussed with the service user.
- The confidentiality of informal carers should be respected and information about them should not normally be disclosed without their consent.

- Where a staff member has dual responsibilities it is important that they explain to the service user at the start of any consultation or assessment in what capacity they are seeing them and the purpose of the consultation or assessment.

5.3.2 Uses beyond the care of the individual

Secondary uses are defined as the use of information for purposes not directly related to the care of an individual 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 and infectious disease reporting.

The Code of Practice on Protecting the Confidentiality of Service User Information states the following[19]:

- All organisations seeking service user information for uses other than direct care should be seeking anonymised or pseudonymised data.
- When the proposed use or disclosure of identifiable information relates to health and social care but is not directly for the care of that service user, the common law requires that the express consent of that service user should normally be obtained.
- 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.
- Organisations should not use personal identifiable information for secondary uses if the service user in question has opted out by specifically refusing consent.
- For all proposed research uses of personal identifiable information, the express consent of the service user should normally be sought. Where consent is being sought this should be by health and social care staff who have a direct relationship with the individual service user.

5.3.3 Other uses

The Code of Practice on Protecting the Confidentiality of Service User Information states the following:[19]

- Consent is not required where there is a statutory obligation to disclose or a discretionary disclosure is justified in the public interest.
- Where a statute, court or tribunal imposes a requirement to disclose information, care should be taken only to disclose the information required to comply with and fulfil the purpose of the law.

- In all cases of discretionary disclosure in the public interest, the test is whether the release of information to protect the interests of a third party exceptionally prevails both over the duty of confidence owed to the service user and the public interest in a confidential health and social care service.[19]

5.4 eHealth developments

There are a number of ehealth initiatives in use in Northern Ireland, including:

- national health identifier (Health and Care number)
- Electronic Prescription Service (ePrescribing)
- Northern Ireland Electronic Care Record (NICER)
- key information summary record.

5.4.1 National health identifier

The Health and Care number (H&C number) uniquely identifies a patient within the HSC in Northern Ireland. It is the equivalent of the NHS number in England and Wales.[77] There is no option to opt-out of this.

5.4.2 Electronic Health Records (EHR)

Plans for the implementation of an EHR are currently underway.[78]

5.4.3 ePrescribing

In 2006, the Department of Health, Social Services and Public Safety (DHSSPS) proposed the introduction of an ePrescribing service. The main aim was to address prescription fraud, which was estimated to have cost the Department £7.8 million in 2004 and 2005. NHS Northern Ireland chose a system where a 2D barcode encodes all information on the paper prescription. This solution was also considered to have minimal impact on prescribers and dispensers. The Electronic Prescribing and Eligibility System (EPES) has been operational throughout Northern Ireland since 1 May 2008. The former Central Services Agency (CSA) stated that it received 16.8 million prescriptions in 2009, all of which could be viewed electronically. The Health and Social Care Business Services Organisation processed more than 41 million prescription items in 2016.[79]

5.4.4 The Northern Ireland Electronic Care Record

The NIECR is a computer system that health and social care staff can use to get information about an individual's medical history that was introduced in 2013. The NIECR contains information 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.[69]

The original consent model in use for the NIECR was informed consent at the point of care. This model has been reviewed by the NIECR Information Governance Workstream, and 'public task' has been agreed as the new legal basis for processing the information within NIECR. This new model takes into account the General Data Protection Regulation, Data Protection Act 2018 principles, the Code of Practice on Protecting the Confidentiality of Service User Information and advice from the Information Commissioner's Office. The option to opt-out of NIECR will no longer be available from 1 March 2020. Key principles are as follows[80]:

- Article 6(1)(e) gives you a lawful basis for processing health data where: "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller" with Article 9(2)(h) identified as the additional condition for processing healthcare data "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".
- Health and Social Care staff access to NIECR will be modelled on the access staff groups currently have to source systems and paper records and what is adequate and relevant to their role in the care team, on a 'need to know' basis.
- The public will be made aware of the proposed use of their data via a NIECR Privacy Notice and updates via the Patient Client Council newsletter.

The NIECR data is generally not used for secondary purposes, although in some cases it is permitted for research and clinical audit. In these cases, there is a specific access form for researchers and access is time bound for 6 months.[78]

NIECR allows access to information to be configured to allow role-based access and control (RBAC). HSC staff are given to right amount of information in line with their role in the care team. In relation to sensitive information such as mental health encounters, specific user groups have been created and assigned to limit who can see that information. This is further explained in table 2.

Table 1: Example roles per level for NIECR

	Level 1	Level 2	Level 3	Level 4
Core data item	Consultants and GPs	Doctors, nurses, midwives, pharmacists, dentists, clinical psychologists	Clinical admin	Health records nurses, midwives
Portal overview	Yes	Yes	Yes	Yes
Care data	Yes	Yes	Yes	No
Medications & allergies	Yes	Yes	Yes	No
Absent patient access	Yes	Yes	Yes	No
Patient search	Yes	Yes	Yes	No
Mental health data (in development)	Yes	Auditable break seal access	No — awareness banner to advise sensitive data exists	No

5.4.5 Key Information Summary Record

If a person has a long-term illness or condition, their GP will decide if it is appropriate for them to have this record. This record allows health and social care staff in Northern Ireland to see details about that patient's health, including medical history and any wishes a patient may have about their treatment. This record includes medical history, agencies involved with the patient, list of care plans, preferred treatment arrangements, resuscitation status and advanced decision to refuse any treatments. This record is stored at a GP's office and is only shared with other health professionals when the patient's consent is given.

5.5 Public engagement

5.5.1 Public engagement in relation to the Northern Ireland Electronic Care Record (NIECR)

In advance of launching the NIECR in 2013, patients, service users and the public were made aware of how data would be shared in the following ways:

- household leaflet drop
- website
- leaflets and posters in point of care locations
- leaflets and posters in libraries
- social media promotion
- press release and press events
- training to HSC clinicians
- information included with all medical cards issued
- a telephone enquiry service.

NIECR moved away from its consent model (in 2019), to the processing of personal health information in the public interest. Steps taken to inform the public of the change in the consent model for include[81]:

- communicating with public by updating their privacy notice
- taking part in a working group to ensure that the public bodies are giving a standardised message to the public regarding chances that have come about following the introduction of GDPR
- consultation with the Privacy Advisory Committee.[82]

5.6 Key learnings

- Northern Ireland has a national health identifier, shared care record (NIECR), and e-prescribing in place. Plans for the implementation of an EHR are currently underway.
- Implied consent is used for the provision of individual/direct care.
- Service users must be informed of what information sharing is necessary for their care.
- Identifiable data can be utilized for uses beyond direct care if required by law or if explicit consent has been obtained. Anonymised data can be used without consent.
- The Northern Ireland Electronic Care Record (NIECR) has moved away from its original consent model and will now process data under the legal basis of 'public task' in order to comply with GDPR. Consent is no longer required to process NIECR data.
- A Code of Practice on protecting the confidentiality of service user information has been developed to provide support and guidance for all those involved in health and social care, concerning decisions about the protection, use and disclosure of service user information.
- Extensive public engagement was carried out when launching NIECR, this included posters and leaflets, social media promotion and training courses for clinicians.

6. New Zealand

New Zealand currently has a population of roughly 4.9 million.[83] It is a parliamentary democracy, an independent country and a constitutional monarchy. The Minister of Health, with the cabinet and government, develops policies and provides leadership for the health and disability sector.[84]

New Zealand has invested significantly in the area of eHealth. New Zealand's progress on interoperability in healthcare is well noted, with standard messaging allowing different care providers to communicate with each other. Patient and provider portals can be made available to healthcare professionals to allow information to be captured at the point of care. This is possible by implementing a range of electronic messages, such as referral and discharge summaries, which covers the exchange of health records from general practitioner (GP) to GP.[85]

eHealth at a glance:

- National health identifier — National Health Index (NHI) number
- Shared care record — implemented regionally by regional governance groups
- New Zealand ePrescription Service (NZePS) — launched in 2018.

Consent model overview:

- Implied consent is used for the provision of individual care; all service users should be informed about how their data will be used.
- Explicit consent is needed for secondary use of the data, unless it has been de-identified or it is required by law for reasons such as to prevent or lessen threat to public health or public safety or the life of an individual.
- Consent is required to use the data for research unless approval is granted by an ethics committee.

6.1 Key organisations

There are a number of key organisations with varying responsibilities in relation to personal health data (collection, use and sharing) in New Zealand. These will be discussed further below:

- the Ministry of Health
- district health boards (DHBs)
- the Privacy Commissioner

- HealthCERT
- Government Chief Data Steward
- Government Chief Digital Officer.

6.1.1 The Ministry of Health

The Ministry of Health leads New Zealand's health and disability system and has overall responsibility for the management and development of that system.

Health Information Governance Guidelines have been developed to provide good practice advice on the safe sharing of personal health information. It provides information on the policies and procedures that are to be implemented to ensure that any health provider who holds health information meets its obligations in terms of the Privacy Act 1993, the Health Information Privacy Code 1994 and other relevant legislation.(86)

A Health Information Security Framework has been designed to support health and disability sector organisations and practitioners holding personally identifiable health information to improve and manage the security of that information. The health and disability sector-wide Health Information Security Framework advises how health information is created, displayed, processed, transported and is disposed of in a way that maintains the information's confidentiality, integrity and availability. Threats concerning the confidentiality, integrity and availability of the health and disability sector's physical and logical assets must be identified, assessed, recorded, prioritised and managed.(87)

6.1.2 District health boards

There are 20 District health boards (DHBs) in New Zealand, and each DHB is governed by a board of up to 11 members. The board sets the overall strategic direction for the DHB and monitors performance. The New Zealand Public Health and Disability Act 2000 sets out the objectives of the DHBs, which include(88):

- improving, promoting and protecting the health of people and communities
- promoting the integration of health services, especially primary and secondary care services
- seeking the optimum arrangement for the most effective and efficient delivery of health services in order to meet local, regional, and national needs
- promoting effective care or support of those in need of personal health services or disability support.

6.1.3 The Privacy Commissioner

The Privacy Commissioner works to develop and promote a culture in which personal information is protected and respected. The Privacy Act applies to almost every person, business or organisation in New Zealand. The Act sets out 12 privacy principles that guide how personal information can be collected, used, stored and

disclosed.[89] The Health Information Privacy Code details 12 Rules for Health Information based on the principles in the Privacy Act.[90]

The Privacy Commissioner's Office has a wide range of functions. All of the Privacy Commissioner's functions are listed in section 13 of the Privacy Act 1993.

Key areas of work include[89]:

- making public statements on matters affecting individual privacy
- investigating complaints about breaches of privacy
- building and promoting an understanding of the privacy principles
- monitoring and examining the impact that technology has upon privacy
- developing codes of practice for specific industries or sectors
- examining new legislation for its possible impact on individual privacy
- monitoring data matching programmes between government departments
- inquiring into any matter where it appears that individual privacy may be affected.

6.1.4 HealthCERT

HealthCERT's role is to administer and enforce the legislation, issue certificates, review audit reports and manage legal issues. It is also responsible for making sure rest homes, residential disability care facilities, hospitals and fertility providers are safe and are at a reasonable standard of service for people who use them as set out under the Health and Disability Service (Safety) Act 2001. [91]

6.1.5 Government Chief Data Steward

The Government Chief Data Steward leads by facilitating and enabling a joined-up approach across government. As well as developing policy and infrastructure, the Government Chief Data Steward provides support and guidance so agencies can use data effectively, while maintaining the trust and confidence of New Zealanders.[92]

The Government Chief Data Steward:[92]

- sets the strategic direction for government's data management
- leads New Zealand's state sector's response to new and emerging data issues
- co-develops a Data Stewardship Framework to enable agencies to manage data as a strategic asset and benchmark their data maturity
- leads the government's commitment to accelerating the release of open data.

6.1.6 Government Chief Digital Officer

The Government Chief Digital Officer is the government functional lead for digital practice and is responsible for[93]:

- setting digital policy and standards
- improving investments
- establishing and managing services
- developing capability
- system assurance (assuring digital government outcomes).

6.2 Legislation

Important legislation in place in New Zealand in relation to the collection, use and sharing of personal health information includes:

- The Privacy Act 1993
- New Zealand Public Health and Disability Act 2000
- Health (Retention of Health Information) Regulations 1996
- Health Information Privacy Code 1994
- The Oranga Tamariki Act 1989 and the Family Violence Act 2018
- The Health Act 1956

Legislation	Description
The Privacy Act 1993	This act provides the general framework for promoting and protecting individual privacy. It does so by establishing principles with respect to the collection, use, disclosure of and access to information relating to individuals. It applies to public and private sector agencies. It also established the role of Privacy Commissioner to investigate complaints about interferences with individual privacy.(94)
New Zealand Public Health and Disability Act 2000	The New Zealand Public Health and Disability Act 2000 introduced a major change to the public funding and provision of personal health services, public health services, and disability support services. It also established new publicly owned health and disability organisations, such as District Health Boards and the Pharmaceutical Management Agency. Section 3(1)(d) describes one of the objectives as being to facilitate access to, and the dissemination of information to deliver, appropriate, effective, and timely services.(95)
Health (Retention of Health Information) Regulations 1996	The Health (Retention of Health Information) Regulations 1996 were introduced to set a minimum period of 10 years for which health information has to be held by health or disability service providers. It also covers the form in which health information is to be retained and the obligations associated with the transferring of health information, for example, when a service provider ceases business.(96)

Health Information Privacy Code 1994	New Zealand has a Health Information Privacy Code in place since 1994. It sets out particular rules for agencies in the health sector, covering health information collected, used, held and disclosed by health agencies and takes the place of information privacy principals for the health sector. The Health Information Privacy Code sets out 12 rules[20]: ▪ **Rule 1, Rule 2, Rule 3 and Rule 4** govern the collection of health information. This includes the reasons why health information may be collected, where it may be collected from, and how it is collected. ▪ **Rule 5** governs the way health information is stored. It is designed to protect health information from unauthorised use or disclosure. ▪ **Rule 6** gives individuals the right to access their health information. ▪ **Rule 7** gives individuals the right to correct their health information. ▪ **Rule 8, Rule 9, Rule 10 and Rule 11** place restrictions on how people and organisations can use or disclose health information. These include ensuring information is accurate and up to date and that it is not improperly disclosed. ▪ **Rule 12** governs how unique identifiers, such as Inland Revenue Department (IRD) numbers, bank client numbers, driver's licence and passport numbers, can be used.
The Oranga Tamariki Act 1989 and the Family Violence Act 2018	From July 2019, new information sharing provisions in the Oranga Tamariki Act[97] and the Family Violence Act[98] enhanced sharing of information between agencies. Four important facts to note about how these acts now work are as follows[99]: ▪ Safety comes first. The sharing of personal information should be considered if there are concerns about someone's safety or if they or others are at risk of harm. ▪ Professionals can proactively share information, and, while in most cases it is not compulsory,

	there will be circumstances where you must share information. ▪ Professionals are protected when they share in good faith and in accordance with the legal requirements. ▪ The Oranga Tamariki Act and the Family Violence Act permit greater sharing than the Privacy Act and the Health Information Privacy Code in some circumstances, but other parts of the Privacy Act and the Health Information Code still apply.
The Health Act 1956	The Health Act 1956 gives the Ministry of Health the function of improving, promoting and protecting public health. It contains specific provisions in section 22 governing the disclosure of identifiable health information by and between health service providers and other agencies with statutory functions. Important sections relating to health information include:(100) ▪ **Section 22C — Disclosure of health information.** This section allows, but does not require, anyone holding health information to disclose that information to requesters from a list of specified agencies, such as a probation officer a social worker or police. The requesters must be seeking the information for the purpose of carrying out their agencies' statutory functions, and disclosure under section 22C is always discretionary. ▪ **Section 22D — Duty to provide health information.** The Minister may at any time, by notice in writing, require any district health board to provide, in such manner as may from time to time be required, such returns or other information as is specified in the notice concerning the condition or treatment of, or the services provided to, any individuals in order to obtain statistics for health purposes or for the purposes of advancing health knowledge, health education, or health research. ▪ **Section 22F — Communication of Information for Diagnostic and other Purposes.** Every person who holds health information of any kind shall, at the request of

the individual about whom the information is held, or a representative of that individual, or any other person that is providing, or is to provide, services to that individual, disclose that information to that individual or, as the case requires, to that representative or to that other person.

- **Section 22H — Anonymous health information.** 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.

6.3 Consent model

6.3.1 Individual care

Implied consent is used for individual care; however, the person must be informed as to why the information is being collected and how it will be used.

The first four rules of the Health Information Privacy Code cover the collection of health information. Health agencies must[101]:

1. **Only collect information they need for a specific purpose —** Rule 1 requires agencies to decide their purposes (how the information is going to be used) before they start collecting information. Once collected for a purpose the information can always be used for that purpose.
2. **Collect information directly from the person concerned, where possible —** Rule 2 makes the patient the first port of call for information about him or herself. It also gives health agencies the opportunity to be open about why they are collecting the information, so the individual can make an informed decision about whether to provide it.
3. **Tell the person concerned why the information is needed, who else will see it and where it will be stored —** Rule 3 lists what health agencies have to tell people when they are collecting health information. This includes the purpose for which the information is being collected, the intended recipients and the agency that will hold the information. This explanation should help people decide what information, if any, to provide to health agencies.
4. **Not be devious, misleading or unnecessarily intrusive in collecting that information —** Rule 4 prohibits health agencies from collecting information unlawfully or unethically. It regulates how information is collected, rather than what is collected.

Disclosure is always allowed when the person concerned or their representative has given their consent or where disclosure was one of the purposes for which the information was originally obtained. In other words, if a doctor collects information from a patient to pass on to a specialist, then there is no need to get the patient's consent for that disclosure because disclosure is one of the reasons for collection and this is allowed by the Health Act 1956. However, the patient would normally have to be told the disclosure was going to occur. Also, even if a patient has given their consent to disclose information about them, the agency holding the information is not required to disclose.(94)

Health agencies can disclose information if this is necessary to avert a serious threat to someone's health or safety. The disclosure must be to someone who can do something about the threat.(94)

A person's representative has a degree of access to, and control over, that person's health information. Disclosure is permitted where a health practitioner discloses the information to a contact person, principal caregiver or relative of the patient in line with 'recognised professional practice' and the patient has not vetoed the disclosure.

6.3.2 Uses beyond the care of the individual

Explicit consent will be required for any use of the information beyond the reason for which it was collected, unless it is allowed by legislation, for reasons such as:(101)

- the information is being used to prevent or lessen threat to public health or public safety, or the life of an individual
- the data is no longer identifiable
- an ethics committee has approved its use for research.

6.3.3 Research

The Health and Disability Ethics Committees (HDECs) are Ministerial committees (established under section 11 of the New Zealand Public Health and Disability Act) whose function is to secure the benefits of health and disability research by checking that it meets or exceeds established ethical standards. HDEC reviews ensure that the use of personal health information for research meets ethical standards. The use of personal health information without consent may be approved by an ethics committee when:

- The process for obtaining that consent is likely to cause undue anxiety for those whose consent is sought or the requirement for consent would prejudice the scientific value of the study or it is impossible in practice to obtain consent due to the quantity or age of the records.
- There would be no disadvantage to the participants or their relatives or to anyone involved in collecting the data.
- The public interest in the study outweighs the public interest in privacy.

Any application for HDEC review must clearly detail how its use of health information meets the legal and ethical requirements.[102]

6.4 eHealth developments

There are a number of ehealth initiatives in use in New Zealand, including:

- national health identifier
- shared care records
- the New Zealand Electronic Prescription Service (ePrescribing).

6.4.1 National health identifier

The national health index (NHI) number is a unique number assigned to patients to help identification when using health and disability services. They have been in use since the 1990s. The New Zealand Health and Information Service is the custodian of the NHI system.[88] There is no option to opt-out of the NHI number.

6.4.2 Shared care record

New Zealand's shared care record is known as the Shared Electronic Health Record. It is a regional shared care record and contains information on medical conditions, allergies, recalls, immunisations, recent test results and prescription medication. Each region has appointed a governance group to ensure the project is implemented and evolves appropriately in each region. The Shared Electronic Health Record is only available to authorised clinical professionals in approved clinical settings. This may include doctors, nurses, pharmacists, paramedics and other clinical staff treating an individual in settings that include[103]:

- afterhours medical centres
- general practices
- community pharmacies
- emergency departments
- other hospital departments
- Wairarapa school clinics.

All authorised users have access to training information and are obliged to be compliant with their organisation's confidentiality, privacy and security policies. Patients can access the My Record portal for information on who has access to the Shared Electronic Health Record in each region.[103]

The consent model in place for the Shared Electronic Health Record is an opt-out system. A patient will automatically have a Shared Electronic Health Record if they are registered at a participating Medical Centre and have not explicitly opted out. They can opt-out of the shared care record either by phone, by post or by contacting their medical centre. They can also choose to withhold some information

if they would like. Some specific health details that may be sensitive will be excluded from being shared on record automatically. If someone decides to opt-out, they can opt back in at any stage. Clinicians must seek a patient's permission before they access the shared care record. It is the responsibility of the patient's GP to inform their patients about the shared care record and to ensure patients are aware that their health information will be available to other clinicians who are authorised to use the shared care record.

The Office of the Privacy Commissioner whose role is to seek to develop and promote a culture in which personal information is protected and respected in New Zealand, released the following recommendations on the secondary use of the Shared Electronic Health Record in 2014. These include:

- Secondary purposes should be minimal and tightly regulated to help maintain clinician and consumer trust. Shared Electronic Health Records hold information on behalf of the clinicians who provided the information and the primary purpose is always to provide high quality care to patients.
- Secondary purposes such as service improvements, teaching, research and audit must be well-publicised and use anonymised or pseudonymised data wherever possible.
- Any new secondary purposes should only be adopted with proper consultation and with careful consideration of the potential risk to public trust in the SCR.
- Users of the SCR should only access the record with patient permission, unless a justification exists for doing so under rule 2 of the Health Information Protection Code.
- All data access and use should be recorded and retained.[104]

6.4.3 e-Prescribing

The New Zealand ePrescription Service (NZePS) provides a secure messaging channel for prescribing and dispensing systems to exchange prescription information electronically. It enables a prescription to be generated by the prescriber, transmitted to the NZePS health information exchange broker, and downloaded electronically at a community pharmacy. Data captured for the prescription service is not generally used for secondary purposes.[105]

A prescriber can note on the electronic prescription that a patient has asked for access to information about a medication to be restricted. Other health professionals will be able to see the restricted information only in an emergency, and will have to give a reason for accessing the information. Access to information will be regularly audited. Patient information is not provided to manufacturers or advertisers.

6.4.4 Future plans

The Ministry of Health has moved away from the idea of building a single electronic health record, towards developing a National Health Information Platform that will enable data about a single patient to be shared. They will focus on joining up data

services to provide information about a patient via the National Health Information Platform. Interoperability is core to the new platform, which will have the ability to assemble a virtual electronic record on an 'as required' basis from multiple trusted sources, and provide access to data and services. The view is to integrate current data sources, accelerating the use of SNOMED, FHIR and other standards. A business case has been developed but has not yet been approved.(106)

6.5 Patient engagement

6.5.1 Data Futures Partnership

The Data Futures Partnership was tasked by the New Zealand Government to draft guidelines which public and private organisations can use to develop a 'social licence' for data use. The Data Futures Partnership resolved that the guidelines must be built on the views of New Zealanders. Over a six week period in February and March 2017, a national engagement programme titled Our Data, Our Way was implemented in response to a brief from the Data Futures Partnership 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. This initiative covered all types of data use; however, the findings are very relevant to healthcare.

Our Data, Our Way 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. These included sharing medical records, education records and data generated by 'smart' street lighting (an example of the Internet of Things).

This engagement with New Zealanders showed that in order for people to feel comfortable about a proposed data use, they first need good information on eight key questions(107):

1. What will my data be used for?
2. What are the benefits and who will benefit?
3. Who will be using my data?
4. Is my data secure?
5. Will my data be anonymous?
6. Can I see and correct data about me?
7. Will I be asked for consent?
8. Could my data be sold?

6.5.2 The Social Investment Agency's Data Protection and Use Policy

The Social Investment Agency is developing a policy to help everyone to easily understand what's appropriate, what's not, and how to do things safely when personal information has a role to play.(108)

Between May and September 2018, the Social Investment Agency held engagements with New Zealanders to find out what they think needs to be included in the Policy. They held 83 hui (this is a term used in New Zealand for social gathering or assembly) and more than 1,000 people participated in the engagement process, including service users (for example, youth and people who use mental health services) non-governmental organisations (NGOs) and government agencies that provide social services. The findings were then published in a report called *What you told us*. The findings of the engagement on the protection and use of data have confirmed the major areas set out for the policy to address as appropriate. The scope of the policy is to[108,109]:

- ensure those receiving social services have a better understanding about how their personal information is collected and used
- clarify when personal identifiable information is needed and what types of personal information should be used for what purpose
- build understanding of what protocols, structures and measures need to be in place to protect personal information
- equip the social sector to work together using information to improve services and make better decisions for New Zealanders
- build understanding, trust, and confidence around the collection, storage and analysis of information.

6.6 Key learnings

- New Zealand has a National health identifier, a shared care record and ePrescribing in place.
- Implied consent is used for the provision of individual care; all service users should be informed about how the data will be used.
- Explicit consent is needed for secondary use of the data, unless it has been de-identified or it is required by law for reasons such as to prevent or lessen threat to public health or public safety, or the life of an individual.
- Consent is required to use the data for research unless approval is granted from an ethics committee.
- An opt-out consent model is in place for the Shared Care Record.
- Important legislation governing the collection, use and sharing of personal health information includes the Privacy Act and the Health Information Privacy Code.
- For ePrescribing, patients can restrict pharmacies from having access to certain data, if they choose to do so.
- The Ministry of Health has moved away from the idea of building a single electronic health record towards developing a National Health Information Platform that will enable data about a single patient to be shared.
- The Data Futures Partnership produced guidelines which public and private organisations can use to develop a social licence for data use. National public engagement was carried out and the findings included eight key questions that must be addressed in order for people to feel comfortable about their data being used.
- The Social Investment Agency carried out an engagement exercise to inform a national policy that will help everyone to easily understand what's appropriate, what's not, and how to do things safely when personal information has a role to play.

7. Ontario (Canada)

Ontario is one of the 13 provinces and territories of Canada and is located in east-central Canada. Ontario has a population of over 14 million.

Canadians have universal coverage for medically necessary healthcare services provided on the basis of need, rather than the ability to pay. Publicly funded healthcare is financed with general revenue raised through federal, provincial and territorial taxation.[110]

The provincial and territorial governments have most of the responsibility for delivering health and other social services funded through health insurance plans. The *Canada Health Act* establishes criteria and conditions for health insurance plans that must be met by provinces and territories in order for them to receive full federal cash transfers in support of health.[110] Ontario Health Insurance Plan (OHIP) is the plan through which the province pays for many health services.[111]

eHealth at a glance:

- Health identifier (Health Card Number) — a unique 10-digit identification number given to eligible residents under the Ontario Health Insurance Plan
- The Electronic Health Record (eHealth Ontario) — an online system that connects hospitals and healthcare settings to show them an integrated view of their patient's health record
- ePrescribing — not yet fully deployed in Ontario; however, many communities are using the PrescribeIT system as their electronic prescription service
- eReferral — development and full implementation is underway and it is already being used by many healthcare providers in Ontario.

Consent model overview:

- Implied consent is used within the 'circle of care'.
- Patients have the ability to withdraw or restrict consent to the sharing of their personal health information via a 'Lock-box' function.
- A record which has been restricted can be accessed in the case of an emergency: this is known as 'break the glass'.
- Identifiable health information can be used for research purposes if research ethics board approval is granted.
- De-identified health information can be used for health research purposes.

7.1 Key organisations

There are a number of key organisations with varying responsibilities in relation to personal health data (collection, use and sharing) in Ontario. These include:

- Canadian Institute for Health Information (CIHI)
- Consent and Capacity Board
- Canada Health Infoway
- the Information and Privacy Commissioner of Ontario (IPC).

7.1.1 Canadian Institute for Health Information (CIHI)

The Canadian Institute for Health Information (CIHI) provides comparable and actionable data and information that are used to accelerate improvements in healthcare, health system performance and population health across Canada. They protect the privacy of Canadians by ensuring the confidentiality and integrity of the healthcare information they hold.(112) CIHI informs policy-makers, supports healthcare management and provides information to Canadians about their health systems and the factors that contribute to good health. Data from CIHI can be extremely valuable to health systems. The data can be used to highlight problems and provides healthcare organisations with the ability to accurately assess and plan healthcare activities.(113)

CIHI is a prescribed entity under subsection 45 (1) of Ontario's Personal Health Information Protection Act (PHIPA). As a prescribed entity, health information custodians may disclose personal health information without consent to CIHI for the purpose of analysis or compiling statistical information with respect to the management of, evaluation or monitoring of, the allocation of resources to or planning for all or part of the health system, including the delivery of services.

A prescribed entity must have in place practices and procedures to protect the privacy of individuals whose personal health information it receives and to maintain the confidentiality of that information. Those practices and procedures must be approved by the Information and Privacy Commissioner of Ontario (IPC/ON) every three years.

CIHI has a comprehensive Privacy Programme that ensures the confidentiality and security of its Canadian healthcare data holdings. Part of this programme is a set of policies governing privacy and security of personal health information. These policies ensure CIHI collects, uses, retains and disposes of personal health information in accordance with applicable laws and data sharing agreements. The program also 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
- initial onboarding mandatory privacy and security training for new employees and annually thereafter, to keep Canadian healthcare information protection matters front and center.(114)

7.1.2 Consent and Capacity Board

The Consent and Capacity Board is an independent body created by the provincial government of Ontario under the Health Care Consent Act. It conducts hearings under the Personal Health Information Protection Act, and other acts. The role of the Consent and Capacity board is the fair and accessible adjudication of consent and capacity issues, balancing the rights of vulnerable individuals with public safety. The board deals with matters of capacity, consent, civil committal and substitute decision making. (115)

7.1.3 Canada Health Infoway

Canada Health Infoway helps to improve the health of Canadians by working with partners to accelerate the development, adoption and effective use of digital health solutions across Canada. Established in 2001, Infoway is an independent, not-for-profit organisation funded by the federal government. Canada Health Infoway conducts research into the benefits of digital health and collects citizens' perspectives of these initiatives. Infoway regularly commissions research, surveys and focus groups to better understand the areas of patient access that need attention. This research highlights important issues for policy and decision-makers to consider as jurisdictions move forward with their consumer health strategies.(116)

7.1.4 The Information and Privacy Commissioner of Ontario

The IPC was established in 1987 and provides oversight of Ontario's access and privacy laws, including the Personal Health Information Protection Act. These laws establish the rules for how Ontario's public institutions and healthcare providers may collect, use and disclose personal health information.

In addition to overseeing the province's access and privacy laws, the IPC also serves both the government and public to:

- resolve appeals when access to information is refused
- investigate privacy complaints related to personal information
- ensure compliance with the acts
- review privacy policies and information management practices
- conduct research on access and privacy issues and provide comment on proposed government legislation and programs

- educate the public, media and other stakeholders about Ontario's access and privacy laws and current issues affecting access and privacy.

The Commissioner is an officer of the Legislature who is appointed by and reports to the Legislative Assembly of Ontario and is independent of the Government of the day.(117)

7.2 Legislation

Ontario has specific laws that govern information access and privacy practices in the province. Important legislation in relation to the collection, use and sharing of personal health information includes:

- Freedom of Information and Protection of Privacy Act and the Municipal Freedom of Information and Protection of Privacy Act
- Personal Health Information Protection Act (PHIPA)
- Personal Information Protection and Electronic Document Act (PIPEDA)
- The Health Care Consent Act.

Legislation	Description
Freedom of Information and Protection of Privacy Act and the Municipal Freedom of Information and Protection of Privacy Act	The purposes of the Freedom of Information and Protection of Privacy Act and the Municipal Freedom of Information and Protection of Privacy Act are the following: ▪ To provide a right of access to information under the control of government organisations in accordance with the following principles: information should be available to the public; exemptions to the right of access should be limited and specific; decisions on the disclosure of government information may be reviewed by the Information and Privacy Commissioner. ▪ To protect personal information held by government organisations and to provide individuals with a right of access to their own personal information.(118)

Personal Health Information Protection Act (PHIPA)

Ontario's health privacy legislation, the Personal Health Information Protection Act (PHIPA), establishes a set of rules regarding personal health information (PHI).

PHIPA gives the public the right to[119]:

- be informed for reasons of the collection, use or disclosure of personal health information
- be notified for theft/loss of unauthorised use or disclosure
- refuse to give consent except in certain circumstances
- withdraw consent by providing notice
- access a copy of your personal health information
- request corrections to your health record
- complain to the Information and Privacy Commissioner if refused access to your record, refused correction or there has been a privacy breach.

The Personal Health Information Privacy Act (PHIPA) is intended to:

- protect the confidentiality, privacy and security of Ontarians' personal health information
- improve quality of care for patients
- provide healthcare practitioners with the right information at the right time
- provide a framework that supports broader healthcare reforms that will modernise Ontario's healthcare system such as Smart Systems for Health
- balance the need to share information in the health sector while protecting individuals' health information privacy
- achieve better health system integration
- Enable improved health system management, performance measurement, and fraud prevention and maximize the benefits of new health technologies.[17]

Personal Information Protection and Electronic Document Act (PIPEDA)	Federal law in Canada states that all organisations covered by PIPEDA must generally obtain an individual's consent when they collect, use or disclose that individual's personal information. People have the right to access their personal information held by an organisation and to challenge the accuracy of the personal information. Personal information can only be used for the purposes for which it was collected and if an organisation is going to use personal information for another purpose, they must obtain consent again. Personal information must be protected by appropriate safeguards.(120) The Ontarian provincial privacy law, PHIPA, has been deemed substantially similar to PIPEDA meaning that PHIPA provides privacy protection that is consistent with and equivalent to that found under PIPEDA. Organisations that are subject to provincial health privacy legislation deemed substantially similar are exempt from PIPEDA with respect to the collection, use or disclosure of personal health information occurring within the respective province.(121)
The Health Care Consent Act	The Health Care Consent Act was enacted in 1996. It establishes the rules for determining capacity in treatment decisions and for obtaining informed, voluntary consent from either the capable patient or his or her substitute decision maker. Where a physician declares a patient incapable of making his or her own treatment decisions, the Act provides for a review process before the Consent and Capacity Board. It also sets out who may be a substitute decision maker and the principles that must be applied when making treatment decisions for an incapable patient.(122)

7.3 Consent model

In Ontario, collection, use and sharing of health information requires either 'implied consent' or 'express consent' (see Table 3).

A health information custodian (HIC) is an institution, facility or private practice health practitioner that has custody or control of personal health information. The HIC is responsible for collecting, using, disclosing, retaining and securely destroying personal health information on behalf of clients. HICs may designate agents to handle personal health information on their behalf for the purposes of providing healthcare. An agent can be an individual or a company that contracts with, is employed by, or volunteers for a HIC.

Consent under PHIPA may be either express or implied, unless PHIPA requires express consent. These consent types are detailed in table 3:

Table 2: Types of consent in Ontario, Canada

Consent type	Definition	Example
Assumed implied consent	May only occur in the context of the 'circle of care'. Unless you have specifically withheld or withdrawn your consent, custodians will assume your implied consent for providing healthcare within the 'circle of care'.(123)	Health information custodians are permitted to disclose personal health information without consent to a medical officer of health if the disclosure is made for purposes of the Health Protection and Promotion Act.(124)
Implied consent	Consent that one concludes has been given based on what an individual does or does not do in the circumstances.(123)	An example of implied consent is consenting to a physician issuing you a prescription; therefore he/she concludes you have implied consent to share your personal health information with the pharmacist.
Express consent	Is given either verbally or in writing, to a custodian to collect, use or disclose your personal health information.(123)	An example of when express consent is needed is the disclosure of information to an organisation that is not the primary holder of the information, for example, insurance company.

7.3.1 Individual care

Assumed implied consent is used when providing individual care. 'Circle of care' is a term commonly used in Ontario to describe the ability of certain health information custodians to assume an individual's implied consent to collect, use or disclose personal health information for the purpose of providing healthcare, in circumstances defined in PHIPA. This 'circle of care' could include doctors, nurses and pharmacists. Consent given by individuals can be withdrawn at any time providing notice is given to the custodian.

Under the Personal Health Information Protection Act (PHIPA), looking at a single healthcare record of a patient if you are not within their 'circle of care' is considered to be a crime. Although PHIPA have not defined the circle of care, 'circle of care' is

easily determined. If a healthcare professional is not directly involved in the care and treatment of the patient, then they are not considered to be part of their 'circle of care' and have no authority to view the individuals patient records.(125)

Infographic: Visual representation of the circle of care.

An individual may, with limited exceptions, withdraw consent at any time for the collection, use or disclosure of personal health information by providing notice to the custodian. A withdrawal of consent would not apply to a collection or use that had already occurred prior to receiving the notice of withdrawal.(126) A consent directive gives patients or their substitute decision makers the option to restrict access to personal health information in the electronic health record. If a patient does not want to the share health information with members of their healthcare team, they can restrict access by asking for a consent directive to be added to their record. This means that when a clinician tries to access their record, a notice pops up indicating that this record is blocked. Even when access is restricted, the health record will not be out of date as new information will continue to be added throughout the patients' healthcare journey. A patient has the option to unblock their record at any time. A patient will receive confirmation once a consent directive is applied or removed.(127)

Everyone is presumed capable of giving consent unless a custodian has reason to believe otherwise. A person is considered capable of giving consent if they are able:

- to understand the information that is relevant to deciding whether to consent
- to appreciate the reasonably foreseeable consequences of giving or not giving consent.

7.3.1.2 'Lock-box' and 'break the glass'

Under PHIPA, individuals may provide express instructions to health information custodians not to use or disclose their personal health information for healthcare

purposes without consent. These provisions have come to be referred to as the 'lock-box' provisions, although 'lock-box' is not a defined term in PHIPA. This means that certain information on their health record is 'masked' and cannot be viewed by healthcare professionals.

The withholding or withdrawal of consent may take various forms, including communications from individuals to health information custodians[128]:

- not to collect, use or disclose a particular item of information contained in their record of personal health information (for example, a particular diagnosis)
- not to collect, use or disclose the contents of their entire record of personal health information
- not to disclose their personal health information to a particular health information custodian, a particular agent of a health information custodian or a class of health information custodians or agents (for example, physicians, nurses or social workers)
- not to enable a particular health information custodian, a particular agent of a health information custodian or a class of health information custodians or agents (for example, physicians, nurses or social workers) to use their personal health information.

'Break the glass' refers to the temporary removal of a consent directive to enable a healthcare provider to access and use the client's personal health information that was previously restricted by a consent directive. Healthcare providers may use the 'break the glass' facility in cases of emergency. Information systems in Ontario allow transparency by providing reports on who accessed what information or when a consent directive was overridden without consent of the client. Processes are in place by which these reports are regularly reviewed and investigated when issues are identified.

7.3.2 Uses beyond the care of the individual

PHIPA sets out a limited set of acceptable uses of personal health information without consent, including, for example, the following purposes[126]:

- planning or delivering programs or services
- risk management, error management or activities to improve or maintain the quality of care or any related program or service
- to a prescribed entity for analysis or compiling of statistical information with respect to the management of, evaluation or monitoring of, the allocation of resources to or planning for all or part of the health system including delivery of services
- obtaining payment or processing, monitoring, verifying or reimbursing healthcare claims

- research, provided that specific requirements and conditions are met
- if permitted or required by law.

A health information custodian may disclose personal health information about an individual:

- to the Chief Medical Officer of Health or a medical officer of health within the meaning of the Health Protection and Promotion Act
- to a public health authority if the disclosure is made for a purpose that is substantially similar to a purpose of the Health Protection and Promotion Act.

Section 30(1) of PHIPA states that health information custodians must not collect, use or disclose personal health information if other information, for example, de-identified information or aggregate information, would serve the purpose of the collection, use or disclosure.(129)

7.3.2.1 Service planning

According to PHIPA, a health information custodian may disclose personal health information about an individual(17):

- for the purpose of determining or verifying the eligibility of the individual to receive healthcare or related goods
- to a person conducting an audit or reviewing an application for accreditation
- to a prescribed person who compiles or maintains a registry of personal health information for purposes of facilitating or improving the provision of healthcare

7.3.2.2 Research

Under clause 37 (1) (j) of the PHIPA, a health information custodian may use personal health information (which the custodian collected for purposes of providing care) only if the custodian prepares a research plan and has a research ethics board approve it.(17)

7.4 eHealth developments

There are a number of eHealth initiatives in use in Ontario, including:

- health identifiers
- electronic health records
- electronic prescription service (ePrescribing)
- eReferral.

7.4.1 Health identifiers

Eligible residents in the province of Ontario may apply to receive provincially funded health services covered by the Ontario Health Insurance Plan. A health card is issued by the Government of Ontario to the insured person. A unique 10-digit permanent identification number and a version code, together known as the health number, are assigned to eligible residents.(130)

7.4.2 Electronic Health Records (EHR)

The electronic health system in Ontario is known as eHealth Ontario. eHealth Ontario is an online system that connects hospitals and healthcare settings to show them their patient's health record. It has a security programme which protects sensitive information. They also conduct threat and risk assessments to ensure that they are adhering to the highest security standards.(131)

The eHealth Ontario electronic health record is a secure and private record of a patient's health history. It gives healthcare teams such as general practitioners, nurses, doctors, emergency staff and specialists real time access to relevant medical information, so that healthcare provided to the patient is based on accurate, up-to-date information. Patients can restrict access to their record by asking for a consent directive to be added to their record as described in Section 7.3.1.2. Currently, patients do not have access to their own health record. However, this is something that is hoped for in the future.(132)

EHealth Ontario is now processing an average of 27.7 million requests for patient information every month. More and more healthcare providers are taking advantage of the ability to access their patients' records on-line. This relieves the burden on patients they treat because they do not to have to remember their clinical history, such as laboratory results, publicly funded prescribed medications and diagnostic images. 99% of hospitals in Ontario and 100% of home and community care organisations are connected to the services.(133)

7.4.3 ePrescribing

ePrescribing has not yet been fully deployed in Ontario.(134) However, PrescribeIT, a national, not-for-profit ePrescribing service for community prescribers in Canada, is now available in Ontario. Physicians and pharmacies in Ontario use PrescribeIT

under the authority of the Health Information Act. They must inform patients about why they are collecting their health information and answer questions about these services, but they are not required to obtain consent from the patient to make health information available to PrescribeIT. Health service providers have a duty under the Health Information Act to consider the wishes of their patients and exercise their professional judgement before deciding how much patient health information is to be made available to these systems. Depending on the patients circumstances, physicians and pharmacists may discuss options with their patient to use a paper prescription or to otherwise restrict access to your health information in their systems.(135)

7.4.4 eReferral

The Ocean eReferral Network is an integrated, cloud-based technology for healthcare referrals developed by CognisantMD. The network includes a map-based, searchable directory of healthcare providers with wait times, intelligent referral forms, end-to-end reporting, and automated status alerts for patients and providers. Using Ocean's secure, online eReferral directory, healthcare providers can search for specialists and patient programs, view wait times and locations, and create and submit a healthcare referral in real time. With integrated electronic medical records (EMRs), referrals are sent, tracked and updated right from the patient's chart.(136)

7.5 Patient engagement

Canada Health Infoway regularly conducts public opinion surveys with Canadians as part of its commitment to listen to their perspectives and understand their needs. The 2018 Connecting Patients for Better Health report provides the latest information on availability; use and citizen interest in accessing their health information online as well as digitally enabled health services (eServices). Some key findings include(137):

- availability of digitally-enabled health services is not meeting the demand of Canadians
- between 7% and 15% of Canadians are accessing their health record online
- there is a growing trend for smartphone use when accessing digital health services.

To further understand the Canadian perspective, Infoway held the Better Health Together Workshop in March 2017. Thirty-four citizen participants from across Canada came together to learn and share their knowledge about digital health. Together, they created the Citizens' Vision for Better Health through Digital Solutions. The vision realised through this workshop was to improve the health of Canadians and to promote true and meaningful collaboration between patients, families, and their healthcare providers through universally accessible, integrated digital technologies. Key principles emerged as part of the workshop.

The participants believed that digital health technology in Canada should be[137]:

- patient and family centred
- ethical
- universal
- integrated
- sustainable
- balanced between evidence and innovation.

7.6 Key learnings

- Ontario has a health identifier and an electronic health record system. There are IT solutions available for providing ePrescribing and eReferral services.
- Implied consent is used within the 'circle of care'.
- Patients can withdraw or restrict consent, which is sometimes referred to as the 'lock-box' function. However, a consent directive can be overridden without the client's consent in the event of an emergency ('break the glass').
- Ontario's health privacy legislation, the Personal Health Information Protection Act (PHIPA), establishes a set of rules regarding personal health information.
- Personal health information can be used and disclosed for research purposes if research ethics board approval is granted.
- De-identified health information can be used for health research purposes.
- Canada Health Infoway regularly conducts public opinion surveys with Canadians and held a citizens' workshop in 2017 to learn and share about digital health.

8. Australia

Australia has a population of over 24 million people, and citizens have access to high standard of healthcare funded mainly through taxation. Australia is comprised of six states and three territories governed by three tiers of government.(138) The three tiers of government are the Australian Government or otherwise known as the commonwealth, state or territory government and local government.(139) Health services in Australia are provided by both public and private sectors. Medicare is Australia's universal health system. Medicare provides free healthcare to all residents and citizens in the public health system.(140)

eHealth at a glance:

- National health identifier — individual healthcare identifiers (IHI) are in place in Australia
- My Health Record is Australia's National Electronic Health Record and is also used by patients to access their health information (patient portal)
- ePrescription was first introduced in early 1990s
- eReferral system in place and is linked to the My Health Record system.

Consent model overview:

- Implied consent is used for the provision of individual care.
- There is an option to opt-out of having a My Health Record and an option to opt-out of identifiable data being used for secondary purposes.
- De-identified data can be used for research and public health purposes unless individuals opt-out via the patient portal.
- The portal has options to delete items and restrict access to personal data.

8.1 Key organisations

There are a number of key organisations with varying responsibilities in relation to personal health data (collection, use and sharing) in Australia, including:

- the Department of Health
- the Australian Institute of Health and Welfare (AIHW)
- the Office of Australian Information Commissioner (OAIC)
- the Australian Digital Health Agency.

8.1.1 The Department of Health

The Department of Health's purpose is to lead and shape Australia's health and aged care systems through evidence based policy, well targeted programs and best practice regulation.(141)

8.1.1 The Australian Institute of Health and Welfare (AIHW)

The Australian Institute of Health and Welfare (AIHW) is a major national agency set up by the Australian Government under the Australian Institute of Health and Welfare Act to provide reliable, regular and relevant information and statistics on Australia's health and welfare. AIHW is an independent corporate Commonwealth entity established in 1987. The AIHW provides statistical information that governments, researchers and the community can use to promote discussion on and improve the delivery of health and welfare for Australians.(142)

8.1.2 The Office of Australian Information Commissioner (OAIC)

The Office of Australian Information Commissioner (OAIC) is an independent statutory agency within the Attorney General's office. The OAIC regulates the handling of health information in an individual's My Health Record and its handling of healthcare identifiers. It also regulates the handling of patient information by healthcare providers.(143)

8.1.3 Australian Digital Health Agency

Tasked with improving health outcomes for Australians through the delivery of digital healthcare systems and the national digital health strategy for Australia, the Australian Digital Health Agency commenced operations on 1 July 2016. It is responsible for national digital health services and systems, with a focus on engagement, innovation and clinical quality and safety. Established as a statutory authority in the form of a corporate Commonwealth entity, the agency reports to state and territory health ministers.(144)

8.2 Legislation

Important legislation in place in Australia in relation to the collection, use and sharing of personal health information includes:

- The Privacy Act 1988
- My Health Records Act 2012
- My Health Record Amendment Bill 2018
- My Health Records Regulation 2012
- Healthcare Identifiers 2010
- My Health Records Guidelines 2016
- The Australian Code for Responsible Conduct.

Legislation	Description
The Privacy Act 1988	The Privacy Act 1988 provides protections around health information handling. This act regulates how organisations collect and handle information and also includes provisions that generally allow and individual to access information held about them. Section 95 of the Privacy Act sets out procedures that Human Research Ethics Committees must follow when personal information is disclosed from a commonwealth for medical research purposes. Section 95A of the Privacy Act sets out a framework for Human Research Ethics Committees to assess proposals to handle health information held by organisations for health research without an individual's consent. They ensure that the public interest in the research activities substantially outweigh the public interest in the procedure of privacy.(145)
My Health Records Act 2012	The My Health Records Act was set up as a basis for the principles on the My Health Record. It has provisions on the role and functions of the system operator. It has a registration framework which entitles individuals such as healthcare providers to participate in the My Health Record system. For example, health information contained in an individual's My Health Record. It also sets the penalties that can be imposed on improper collection, use and disclosure of information. The Commonwealth Minister for Health can make My Health Record rules under section 109 of the Act about matters required or permitted in the Act to be dealt with by that rule. Some rules set up under the Act to date are(146): ▪ My Health Record Rule 2016: This specifies requirements for registered entities in the system, that is, operations, security. ▪ My Health Record Rule 2015: This specifies requirements for registered healthcare providers that assist individuals to register. ▪ My Health Record Rule 2017: Provides national implementation of the My Health Record system opt-out.

My Health Record Amendment Bill 2018	On 26 November 2018, Australian Parliament passed this bill. The new laws meant that the principles contained within the framework to guide the secondary uses of data will become law. A data governance board will be established to approve the release of any data in line with these rules. This also removes any ability for insurers to access this data for the purpose of research.(147)
My Health Records Regulation 2012	This is used for identifying information and privacy laws that continue to apply to the disclosure of sensitive information.(146)
Healthcare Identifiers 2010	This provides additional detail and requirements regarding the operation of the healthcare identifiers service.(146)
My Health Records Guidelines 2016	These guidelines set out the Information Commissioners approach to exercising its enrolment and investigate powers under the My Health Record System.(147)

8.2.1 The Australian Code for Responsible Conduct 2018

Developed jointly by the National Health and Medical Research Council, the Australian Research Council and Universities Australia, the 2018 Code has broad relevance across all research disciplines. It articulates the broad principles that characterise an honest, ethical and conscientious research culture. The Code sets out principles and responsibilities that both researchers and institutions are expected to follow when conducting research. The code does not incorporate laws however; it is more of a guide to research conduct behavior. The principles that are hallmarks for of research conduct are(148):

- Honesty in the development, undertaking and reporting of research.
- Rigor in the development, undertaking and reporting of research.
- Transparency in declaring interests and reporting research methodology, data and findings.
- Fairness in the treatment of others including fellow researchers and others involved in the research.
- Respect for research participants, the wider community, animals and the environment.
- Recognition of the right of Aboriginal and Torres Strait Islander people to be engaged in research that affects or is of particular significance to them.

- Accountability for the development of research including complying with legislation.
- Promotion of responsible research practices.

8.3 Consent model

8.3.1 Individual care

The My Health Record system is the Australian Government's electronic health record system. A My Health Record was created for every individual in Australia in January 2019, unless they had opted out in advance. Individuals can choose to opt-out of having a record at any time. Consent is implied for primary use of data, but individuals have options to opt-out or to delete documents or limit access to their record via the portal.(149)

An online portal is available to those who have a My Health Record. Using this portal, individuals can control privacy by limiting who has access to their record.

Individuals can choose to invite a nominated representative to access their My Health Record. A nominated representative might be a family member, close friend, or carer.(150)

Individuals can decide which healthcare providers can view their record by setting a record access code (RAC). Once a record access code is shared with a healthcare organisation, such as GPs or specialists, they will be able to access the record. Healthcare organisations can be removed from the provider access list at any time.(150)

There are two ways to control access to specific health documents in My Health Record(150):

- Restricting a document to prevent healthcare providers and nominated representatives viewing certain information.
- Removing a document so that only the patient and the professional who added it to your My Health Record can see it.

Healthcare providers can still view restricted documents in an emergency. A medical emergency involves a serious threat to your health, life or safety.(150)

It should be noted that some people may not have the technical skills or capacity to access these options on the portal, and this may be a barrier to them having full control of their record.(151)

8.3.2 Uses beyond the care of the individual

The My Health Record Act provides that unauthorised collection, use or disclosure, as well as secondary disclosure, of health information in a person's My Health

Record is a breach of the My Health Record Act and an interference with privacy (sections 59 and 60).[146] However, where My Health Record data has undergone an appropriate and robust de-identification process, it is not considered health information and is therefore not subject to the My Health Record Act or Privacy Act. It is also important to note that My Health Record data which has not been properly de-identified could be considered health information due to the risk of re-identification.

My Health Record data is currently not being used for secondary purposes. It is hoped that the data will be available for secondary uses by 2020, at which point secondary use will be governed by the Framework to Guide the Secondary Use of My Health Record System data.[152] Patient consent is required in order to release individual identifiable data for secondary purposes.[153]

The My Health Record Amendment was passed in 2018. The new laws meant that the principles contained within the framework to guide the secondary uses of data will become law.[147]

The development of the framework was informed by a national public consultation process. The purpose of the framework is to inform Australians about how My Health Record system data may be used for secondary purposes. There are also other limited circumstances in which a consumer's My Health Record information may be used under the My Health Records Act, including for court proceedings, coronial investigations and law enforcement purposes, and to enable the system operator to run the My Health Record system effectively (such as to undertake investigations and audits).

The framework describes the governance mechanisms and technical processes to be implemented before data can be released for research, policy and planning secondary purposes. Key principles include[152]:

- Individuals can choose to have a My Health Record but elect for the information in it not to be used for secondary purposes.
- My Health Record system data cannot be used solely for commercial and non-health related purposes.
- The provision of My Health Record system data to insurance agencies will not be permitted.
- The use of My Health Record system data for clinical trials recruitment will not be considered until an explicit consent option is available in the system access controls.
- Custodianship for the secondary use of My Health Record system data rests with the Australian Institute of Health and Welfare.
- Applications for My Health Record system data will be assessed by a Data Governance Board, comprising representatives from the AIHW, the Australian

Digital Health Agency (as the system operator) and a range of independent experts, including representatives from population health/epidemiology, research, health services delivery, technology, data science, data governance and privacy, and consumer advocacy.

- The Board will consider applications for the secondary use of de-identified My Health Record system data, as well as identified data with the consent of the healthcare recipient.
- The Board will regularly reconsider the privacy protection processes around secondary use of My Health Record system data. Particular consideration will be given to circumstances where there is already data in the public domain about individuals.

8.4 eHealth developments

There are a number of ehealth initiatives in use in Australia, including:

- national healthcare identifiers
- electronic health records (My Health Record)
- electronic prescription service (ePrescribing)
- eReferral.

8.4.1 National health identifier

Individual Healthcare Identifiers are automatically assigned to all individuals registered with Medicare Australia or enrolled in the Department of Veterans' Affairs (DVA) programs. Those not enrolled in Medicare Australia or with the Department of Veterans' Affairs are assigned a temporary number when they next seek healthcare. This number is then validated by the Healthcare Identifiers (HI) Service Operator and becomes their unique Individual Healthcare Identifier.(154) There is no option to opt-out of the Individual Healthcare Identifier.

8.4.2 Electronic health record — My Health Record

The My Health Record system is the Australian Government's digital health record system. It contains My Health Records, which are online summaries of individuals' health information, such as medicines they are taking, any allergies they may have and treatments they have received. A My Health Record allows an individual's doctors, hospitals and other healthcare providers (such as physiotherapists) to view the individual's health information, in accordance with their access controls. Individuals are also able to access their record online.(149) The My Health Record contains health information relating to the individual, including:

- an overview of the individuals health record
- hospital discharge summaries
- reports from test and scans, such as blood tests
- prescribed medications

- referral letters.

The My Health Record system is managed in line with the Australian Government Protective Security Policy Framework. My Health Record data is stored in Australia, and is protected by high grade security protocols to detect and mitigate against external threats. Design features include many safeguards to protect the information stored within the system, including audit trails, technology and data management controls, as well as appropriate security measures to minimise the likelihood of unauthorised access to information in a patient's record. In addition to these measures, the My Health Record system is protected by legislation which governs the way the system is accessed, managed and used.(155)

Australia previously attempted to introduce an electronic health record (EHR) in 2012 called the Personally Controlled Electronic Health Record. This was an opt-in model for both patients and professionals. Unfortunately, it was not a success due to poor opt-in rates as well as lack of uptake and utilisation. Following on from this, the My Health Record was launched in 2018, with an opt-out system in place.

8.4.3 ePrescribing

In Australia, ePrescribing systems in general practice were first developed in the early 1990s. The uptake of e-prescribing systems was accelerated in 1999 because of Commonwealth government incentive payments of $10,000 to practices that acquired an email address and used ePrescribing software to write the majority of their prescriptions. Currently, over 90% of general practitioners use one of the 20 or so commercial systems that are available to write prescriptions, order pathology and other tests, record medical progress notes or communicate with other healthcare providers. Despite the widespread use of ePrescribing systems, there are no clear standards or guidelines for their development.(156)

8.4.4 eReferral

The My Health Record system supports the collection of eReferrals. When a healthcare provider creates an eReferral, it will be sent directly to the intended recipient, as per current practices. A copy may also be sent to the My Health Record system. eReferrals can be sent and received directly between healthcare providers (point-to-point), through secure messaging, and or uploaded to and retrieved from a patient's My Health Record (point-to-share).(157)

8.5 Patient engagement

From March to October 2016, trials of different participation arrangements for My Health Record were run. The aim of the trials was to understand consumer reaction to different participation arrangements, as well as healthcare provider usage and upload of clinical information to the patients' records, when most of their patients have a My Health Record.[23]

The trials were conducted as a collaboration between the Department of Health, Primary Health Networks, the state health departments and relevant hospital and health services. An independent evaluation of the trials commissioned by the Department of Health was conducted by Siggins Miller Consultants to look at the outcomes from these trials. Key findings included[23]:

- An opt-out system resulted in greater participation
- there was a high level of support for the automatic creation of a My Health Record for every individual
- people had fewer concerns about My Health Record once the benefits were explained to them
- the overall level of awareness and understanding was low
- the majority of people thought that healthcare providers should not be able to opt-out of using the My Health Record and that the government should make use compulsory for healthcare providers.

8.6 Key learnings

- Australia is using national health identifiers, electronic health records, ePrescription and eReferral
- Implied consent is used for the provision of individual care.
- There is an option to opt-out of having a My Health Record.
- There is an option to opt-out of identifiable data being used for secondary purposes.
- De-identified data will be used for research and public health unless you opt-out via the portal.
- The portal has options to delete items and restrict access to personal data.
- My Health Record data is currently not being used for secondary purposes. It is hoped that the data will be available for secondary uses by 2020, at which point secondary use will be governed by the Framework to Guide the Secondary Use of My Health Record System data.
- Key pieces of legislation have been introduced as a basis for the principles on the My Health Record, including the use of My Health Record Data for primary and secondary uses.
- Australia launched an EHR in 2012 which was opt-in for both patients and professionals, this was not successful due to poor opt-in rates and the My Health Record was launched in 2018, using an opt-out system.
- In 2016, trials of different participation arrangements for My Health Record were run. The trials tested different opt-out and opt-in arrangements in different areas. The trials found that the opt-out system resulted in greater participation.

9. Estonia

Estonia currently has a population of roughly 1.3 million and has one of the leading eHealth solutions in Europe.[158,159] The Estonian healthcare system is mainly publicly funded through solidarity-based mandatory health insurance contributions in the form of an earmarked social payroll tax.[160]

The Estonian National Health Information System (ENHIS) is a national central electronic database for processing health records of all patients receiving healthcare services from any Estonian healthcare service provider. The ENHIS has been functioning since 1 September 2008.

eHealth at a glance:

- Estonia uses national health identifiers — Personal Identification Code (PIC).
- Electronic health record — the Estonian National Health Information System (EHNIS)
- Estonia has an online patient portal — www.digilugu.ee
- ePrescription services are in use in Estonia
- eReferral — used by all family doctors and specialists working in larger healthcare institutions throughout Estonia
- Emergency services — eAmbulance operate in Estonia and patient's ID codes can be used to read real time-critical information, for example, blood type/allergies
- eConsultation was set up in 2013.

Consent model overview:

- Implied consent is used for the provision of individual care.
- Patient consent is not needed for creating EHRs or for processing EHRs for the purpose of providing healthcare.
- Explicit consent is required if data is used outside the organisation in which it was collected.
- Electronic health information can only be used/provided to licensed healthcare professionals.
- Estonians can opt-out of having their health information stored on the central database and can deny specific providers access to their data.
- Secondary use of personal health information is allowed if a permit has been issued by the data protection inspectorate.
- Anonymised data can be used for research and planning purposes.

9.1 Key organisations

There are a number of key organisations with varying responsibilities in relation to personal health data (collection, use and sharing) in Estonia, including:

- Ministry of Social Affairs
- Health and Welfare Information System Centre (HWISC) (previously the Estonian e-Health Foundation (EHF))
- the Republic of Estonia Information System Authority
- Data Protection Inspectorate

9.1.1 Ministry of Social Affairs

The Ministry of Social affairs is responsible for organisation, coordination and implementation of eHealth projects as well as the administration and development of the ENHIS, standardisation of medical databases and classifications, and their integration in the healthcare system. The ministry is responsible for policy and strategy while the Health and Welfare Information System Centre (HWISC) manages the daily administration of the ENHIS. The data controller for the ENHIS is the Ministry of Social Affairs. The HWISC is the organisation authorised to process data.(161)

9.1.2 Health and Welfare Information System Centre

The Health and Welfare Information System Centre (HWISC) is a department of the Ministry of Social Affairs. From the perspective of ENHIS, it promotes and develops national e-solutions within the healthcare system. This includes:

- Developing and managing the health information system, which consists of eHealth cross-national projects, including in the following areas:
  - electronic health record
  - digital registration
  - digital image
  - digital prescription
  - eConsultation
  - a statistics module
  - eAmbulance.
- Standardisation — responsible for national development and administration of classifiers and standards as well as the creation of electronic documents, translation and harmonisation of terminology
- Developing the organisation — creating cooperation partnerships with parties in Estonia as well as in Europe, initiating new projects and participating in cooperation projects, informing the society about health related topics as well as supporting individual development of the members of the organisation.(162)

It is the centre of information and communication technology in health, social protection and labour field. The main responsibilities include:(163)

- development of information systems, standards, databases and eServices
- maintenance of services and infrastructure
- providing information security
- data analysis to support policy making, reporting, productivity monitoring and supervision.

9.1.3 The Republic of Estonia Information System Authority

The Republic of Estonia Information System Authority leads the development of national IT systems and ensures national cybersecurity. They are committed to ensuring the smooth and sustainable operation of a secure e-state. They manage and protect the state internet network and ensure secure e-elections. They aim for a sustainable digital identity of Estonia and its wide use around the world. By managing the State Portal eesti.ee, they deliver citizens important information regarding the state. The reliability and development of the digital state depend on them. They increase confidence in the state and its services.

X-Road is the backbone of e-Estonia. It is software that is a 'centrally governed distributed integration layer between information systems', with its first iteration developed and launched by Estonia's Information System Authority in 2001. It allows the nation's various public and private sector e-service information systems to link up and function in harmony.(164)

9.1.4 Data Protection Inspectorate

The Estonian Data Protection Inspectorate is the national supervisory authority of data protection. Health data, including EHRs, fall in the scope of sensitive personal data for which additional regulatory requirements are applicable. Estonian Data Protection Inspectorate supervises whether health data, including EHRs, are processed in compliance with rules for sensitive personal data protection.(161)

9.2 Legislation

In Estonia there are a number of pieces of legislation in place in relation to the collection, use and sharing of personal health information, including[161]:

- The Health Services Organisation Act, 2001
- The Personal Data Protection Act, 2007
- The Regulation on the System of Security Measures for Information Systems 2007
- The Law of Obligations Act, 2001
- The Regulation on Conditions and Procedure for the Issue of Prescriptions for Medicinal Products and for the Dispensing of Medicinal Products by Pharmacies and the Format of Prescriptions 2005
- The Penal Code, 2001

Legislation	Description
The Health Services Organisation Act, 2001	Chapter 5 of the Health Services Organisation Act of 9 May 2001 establishes the most general regulatory requirements for the functioning of the ENHIS. It is also the basis for enforcing the government regulations concerning the ENHIS. This act: ▪ defines the ENHIS ▪ establishes general principles for forwarding data to the ENHIS and granting access to ENHIS data ▪ establishes the ENHIS ethics committee. The regulation does not contain data protection rules, but refers to the Personal Data Protection Act.[161]
The Personal Data Protection Act, 2007	The Personal Data Protection Act of 15 February 2007 applies as a general law to all personal data protection issues related to EHRs. The Data Protection Inspectorate monitors compliance with the Personal Data Protection Act and guidelines issued by the Inspectorate are useful in interpreting the Act. For example, guidelines on processing personal data in scientific research have been issued by the Inspectorate.[161]

The Regulation on the System of Security Measures for Information Systems	The Regulation of 20 December 2007 on the System of Security Measures for Information Systems establishes security classes for information systems. The security class of ENHIS is also established on the basis of this regulation.(161)
The Law of Obligations Act, 2001	The Law of Obligations Act of 26 September 2001 provides for the general regulatory requirements of the provision of healthcare services agreement. It establishes the confidentiality obligation of the professionals, healthcare service providers and the obligation to document the provision of healthcare and the liability of healthcare service. It also provides the legal principles for the civil liability of the providers of medical services. Estonian legislation does not currently regulate or prescribe a more specific legal regime for the liability related to the use of EHR systems. Therefore, the general principles for negligence/malpractice apply.(161)
The Regulation on Conditions and Procedure for the Issue of Prescriptions for Medicinal Products and for the Dispensing of Medicinal Products by Pharmacies and the Format of Prescriptions	Digital prescriptions are regulated under Regulation of 18 February 2005 on the Conditions and Procedure for the Issue of Prescriptions for Medicinal Products and for the Dispensing of Medicinal Products by Pharmacies and the Format of Prescriptions. This regulation establishes:(161) ▪ The conditions and procedure for the issue of prescriptions for medicinal products and for the dispensing of medicinal products on the basis of prescriptions or order forms, including for the preservation and registration of medical prescription forms, order forms and accompanying documents. ▪ The format of prescriptions. ▪ The conditions and procedure for the dispensing of medicinal products on the basis of the prescriptions of the EU Member States, EEA Member States and the Swiss Confederation.
The Penal Code, 2001	The Penal Code of 6 June 2001 prescribes criminal liability for confidentiality breaches and the State Liability Act of 2 May 2001 provides the basis or

	claiming compensation if rights are violated in the process of performance of a public duty.(161)

Estonia has been strongly recognised as a leader in the eGovernance landscape in Europe by implementing complementary legal frameworks protecting privacy in order to promote the usage of eServices.(165)

9.3 Consent model

9.3.1 Individual care

Patient consent is not required for the purpose of creating EHRs or for the provision of healthcare. However, Estonian law has established an opt-out system for the sharing of EHRs in the ENHIS whereby the patient can prohibit sharing of their personal health information in the ENHIS with healthcare providers. To do that, the patient can opt-out using the My E-Health platform (patient portal) online application. As an alternative, the patient must submit an application to his or her healthcare provider (to prohibit access to ENHIS data connected to that provider) or to the Ministry of Social Affairs (to prohibit access to all personal data in the ENHIS). If the application is submitted to the healthcare service provider, it must be in written form. If the application is submitted to the Ministry of Social Affairs, it can be submitted online on the patient platform 'My E-Health.' Identification of the patient is confirmed through logging in with the national Identity Card or through mobile phone based identification (mobile-ID).

On the My E-Health platform, the patient has several options[161]:

- deny healthcare professionals access to all data on the ENHIS
- restrict access to certain information on the ENHIS
- grant access to his or her ENHIS data to other persons, for example family members.

9.3.2 Uses beyond the care of the individual

Consent is required when using personal health information for other purposes other than direct care; Estonian citizens are protected against their personal information being processed without permission. It is mainly regulated by the Health Services Organisation Act and Personal Data Protection Act. The requirement for consent for secondary use of EHR data depends on whether the data are anonymised or not. If the data are anonymised, it is not considered to be personal data and thus the general requirements of the Personal Data Protection Act do not apply. If information is not anonymised, the data can only be used for secondary use if a permit has been issued by the Data Protection Inspectorate.[161]

When an Estonian citizen gives consent to the use of his or her personal information, there are seven important legal principles laid out in the Personal Data Protection Act that a data processor must follow[166]:

1. **Principle of Legality —** The personal data of an individual will only be collected in an honest and legal manner.
2. **Principle of Purposefulness —** Personal data will only be collected for achieving determined and lawful objectives and will not be processed in a manner not conforming to objectives of data processing.

3. **Principle of Minimalism —** Personal data will only be collected to the extent necessary for achieving determined purposes.
4. **Principle of Restricted Use —** Personal data will be used for other purposes only with the consent of the data subject or with the permission of the competent authority.
5. **Principle of High Quality of Data —** Personal data will be up-to-date, complete and necessary for the achievement of the purpose of data processing.
6. **Principle of Security —** Security measures will be applied in order to protect personal data from involuntary or unauthorised processing, disclosure or destruction.
7. **Principle of Individual Participation —** The data subject will be notified of data collected concerning them. Furthermore, the data subject will be granted access to data concerning them and the data subject has the right to demand the correction of inaccurate or misleading data.

9.3.3 Research

Consent is needed for processing of personal health information. However, as described in Section 9.3.2, secondary use of personal health information is allowed without consent if a permit has been issued by the data protection inspectorate. Anonymised (coded) health data is not personal data and can be used for scientific research or official statistics without the consent of the patient. There is therefore no opt-out system in this regard.(161)

9.4 eHealth developments

There are a number of ehealth initiatives in use in Estonia, including:

- national health identifier
- electronic health records
- ePrescribing
- patient portal
- eReferral
- eAmbulance
- eConsultation
- X-Road (interoperability e-solution).

9.4.1 National health identifier

The Personal Identification Code (PIC) is a unique 11-digit number assigned by the state and used for citizens and residents in eGovernment services, including health. Further authentication processes are completed in connection to the Estonian eID. This mandatory national card provides digital access to all of Estonia's secure e-

services, for example, proof of identification when logging into bank accounts, i-voting, to check medical records, submit tax claims and to use ePrescriptions.(167)

9.4.2 Electronic Health Records (EHR)

The Estonian National Health Information System (EHNIS) has been in operation since 2008. Healthcare providers are connected to the health information system and patient health data is stored centrally. There are more than 20 million different health documents (such as case summaries, referrals, vaccinations, dental information and medical images) and over 250 million events stored in the health information system. As the fundamental principle in Estonian eGovernance state, this type of data belongs to the citizen concerned. Health data and healthcare eServices are accessible to patients through the patient portal www.digilugu.ee.

Overview of the national laws on electronic health records in the EU Member States — National Report for the Republic of Estonia indicates that that hospitals strictly regulate employees who can access EHRs and ENHIS and under what conditions.(161) Hospitals take any infringement of such internal rules very seriously and have issued warnings or ended employment contracts with employees who have accessed EHRs without authorisation. All activities on ENHIS are recorded and every access can be tracked down.

The six main principles of security of Estonian Health Information system are:

- a secure authentication of all users with ID-card or Mobile ID
- digital signing or stamping of all medical documents
- maximum accountability and transparency — all actions will leave an unchangeable (and un-removable) secure trail, protected by blockchain
- coding of personal data — separating of personal data from medical data
- encrypted database that removes the confidentiality risk from the technical administrators
- monitoring of all actions together with the corresponding counter measures (both organisational and technical).(168)

9.4.3 Patient portal

One of the crucial parts of ENHIS is the patient portal. Patients can log into the patient portal (www.digilugu.ee) using their national ID card or mobile ID. Using the patient portal, the user can:(161)

- log in with ID card or mobile ID
- view and update personal data
- add contact data of close relatives
- view their medical data from healthcare providers
- view electronic referral letters and electronic prescriptions

- add representatives for themselves for actions such as collecting ePrescriptions
- make declarations of intent (for example donation of organs)
- access health insurance data
- hide sensitive health data from doctors and representatives
- complete a health declaration form before an appointment
- view the log of who has accessed their data.

9.4.4 ePrescribing

ePrescription is a centralised paperless system for issuing and handling medical prescriptions. Most recent figures indicate that 99% of all prescription medicine issued to Estonian patients is done by digital prescription. This is a very efficient system connecting every hospital and pharmacy in Estonia, cutting down on paperwork and doctor visits and saving untold amounts of time and effort. Doctors can prescribe medicine electronically and all patients can obtain their prescriptions at any pharmacy by presenting their ID Card. This enables the pharmacist to retrieve the patient's information from the system and prepare the prescription. This was a Digital Prescription project developed by the Estonian Health Insurance Fund.(169)

9.4.5 eReferral

eReferral is part of the nation-wide EHR system services in Estonia. Patients need a family doctor's referral in order to see most specialists and to be admitted as a nonemergency inpatient. A digital referral (eReferral) is a message sent to a specialist via the health information system. With it, the doctor submits patient health information and justifies the need for the referral. eReferral is used by all family doctors and specialists working in larger healthcare institutions throughout Estonia. Patients can also view digital referrals in the national Patient Portal www.digilugu.ee. Patients are only able to book an appointment with a specialist after a doctor has submitted a digital referral to the health information system (ENHIS). The patient can then make an appointment by the website of the medical institution, by calling reception or on site. In all three cases, the referral will be stored in the health information system (ENHIS).(170)

9.4.6 eAmbulance

eAmbulance is another eHealth initiative in Estonia. This is a quick-response solution that can detect and position the phone call for the ambulance within 30 seconds and quickly sends the ambulance to the necessary location. In an emergency situation, a doctor can use a patient's ID code to read time-critical information, such as blood type, allergies, recent treatments, on-going medication or pregnancy.(171)

9.4.7 eConsultation

An eConsultation service was set up in by the EHIF in Estonia in 2013. This service enables family physicians to quickly and conveniently consult with a specialist to

clarify their patient's diagnosis and prescribe treatment. In the beginning only the specialties of urology and endocrinology provided eConsultation services, but over the years the use of the service has increased among family physicians and several dozen new specialties have been added to the service.(172)

9.4.8 X-Road

X-Road is an eSolution that allows the nation's various public and private sector databases to link up and function in harmony.(158)

9.5 Patient engagement

Estonia has one of the most advanced eGovernance systems in the world. Many services require the public to use eSolutions when accessing public services, from voting to accessing healthcare. For this reason, Estonia has undertaken a number of initiatives to reduce the digital divide by increasing access to the Internet. Technological literacy should be a key step in a governments approach to progressing eGovernance and eHealth solutions at a national level. An example of this is the Come Along! campaign initiated in 2010, to improve Internet literacy, free of charge with training and informational sessions targeting 100,000 citizens in Estonia.(173)

When Estonia began the implementation of e-health initiatives in the 1990s, a large investment was made in the area of public relations, legal and ethical discussions and education.(174) This highlights how important patient engagement and building trust is at the beginning of an eHealth journey. Public trust promotes confidence in eHealth services and increases engagement with eHealth initiatives.

9.6 Key learnings

- Estonia has national health identifiers (Personal Identification Code), electronic patient records (stored centrally in the Estonian National Health Information System (EHNIS)), patient portal, ePrescription, eReferral, eAmbulance and eConsultation services.
- Estonia is recognised as a leader in eHealth, implementing complementary legal frameworks that protect privacy in order to promote the usage of eServices.
- Patient consent is not needed for creating EHRs or for processing EHRs for the purpose of providing direct healthcare.
- Estonians can opt-out of having their health information stored on the central database and can deny specific providers access to their data.
- Explicit consent is required when processing personal health information for purposes other than direct care.
- Secondary use of personal health information is allowed if a permit has been issued by the data protection inspectorate or if the data is anonymised.
- Patients have access to an online portal where they can view and update personal data, add information, view their medical records, make declarations of intent, hide sensitive data and view a log of who has accessed their data.
- X-Road is an e-solution that allows the nation's various public and private sector databases to link up and function in harmony.
- Estonia uses blockchain technology to ensure high levels of information security.

10. Finland

Finland currently has a population of approximately 5.5 million.[175] It ranks among the three strongest health technology economies in the world.[176] Finland is divided into some 311 municipalities. Each municipality is responsible for arranging healthcare for its inhabitants. Secondary care is arranged by 21 hospital districts, of which 20 are in mainland Finland and one on the Åland Islands. Finland's healthcare sector is primarily funded by tax and state contributions. Public healthcare is supplemented by privately funded occupational healthcare that covers 1.9 million workers and private clinics.

eHealth at a glance:

- Health identifier - Finnish National ID Number
- Kanta services are the national centralised integrated and shared electronic data system services for healthcare and social welfare
- The Kanta services include:
  - My Kanta Pages
  - Prescription services
  - Pharmaceutical database
  - Patient data repository

Consent model overview:

- Consent is not needed for the collection of personal health information as public healthcare organisations are obliged to enter patient records in a nationally centralised integrated and shared repositories.
- Implied consent is used in the provision of individual care within the healthcare provider a patient attends.
- Explicit consent is needed if information is shared with external healthcare providers. Patients can give consent at point of care or online through My Kanta Pages.
- Secondary use of personal health information is allowed if a permit has been issued by the Social and Health Data Permit Authority (Findata).
- Health information should always pseudonymised or anonymised when shared for research or planning purposes unless a permit has been granted from the data permit authority.

10.1 Key organisations

There are a number of key organisations with varying responsibilities in relation to personal health data (collection, use and sharing) in Finland, including:

- the Finnish Institute for Health and Welfare (THL)
- the Social Insurance Institution of Finland (Kela)
- the Office of the Data Protection Ombudsman (TSV)
- the Social and Health Data Permit Authority (Findata)

Other organisations include the Ministry of Social Affairs and Health (STM), the Population Register Centre of Finland (VRK), the Finnish Medicines Agency (Fimea), the National Supervisory Authority for Welfare and Health (Valvira), the Regional State Administrative Agencies (AVI), healthcare service providers (public primary healthcare centres, public hospitals districts, public and private hospitals, private healthcare providers) and social welfare service providers (public and private actors).

10.1.1 The Finnish Institute for Health and Welfare

The Finnish Institute for Health and Welfare (THL) is a research and development institution whose purpose is to promote the wellbeing and health of the population, to prevent diseases and social problems and to develop social welfare and healthcare services. The THL executes its remit through research, monitoring and evaluation, development, expert opinions, official duties and international cooperation. It is the official compiler of statistics in its sector and manages the collection and leveraging of the data within its domain. It gathers and produces information based on research and register data which can be used to support decision-making.

The THL serves various parties: the government, municipal and provincial decision-makers, actors in the social welfare and health sector, organisations, the research community, and the public. It is an independent expert agency working under the Ministry of Social Affairs and Health. The THL work focuses on[177]:

- sustainability of the social welfare
- reducing inequality and social exclusion
- monitoring trends in diseases
- preparing for health threats
- transformation of the health service system.

In addition to these focus areas the THL is responsible for the concepts and functional requirements for the Kanta services and national data structures, classifications and interoperability specifications for the social and healthcare sectors, for example, SNOMED-CT and CDA R2 schemas. The THL is also responsible for national registries and statistics for the social and healthcare sectors.

10.1.2 The Social Insurance Institution of Finland

The Social Insurance Institution of Finland (Kela) provide basic social security for all persons resident in Finland throughout the different stages of their lives as defined in the legislation.(178) Kela runs the statutory national health insurance scheme that covers all residents in Finland and includes outpatient medication reimbursement, reimbursement of medical costs in the private sector, compensation of travel costs to healthcare units, sickness allowance, maternity leave allowance and compensation for some rehabilitation services and reimbursement. In addition to these services, the Kela has overall responsibility for the technical implementation and operation of the national centralised integrated and shared Kanta services.

10.1.3 The Office of the Data Protection Ombudsman

The Office of the Data Protection Ombudsman is an independent authority appointed by the government to oversee the compliance of organisations with data protection legislation. The Data Protection Ombudsman safeguards the rights and freedoms of individuals with regard to the processing of personal data. The ombudsman covers all aspects of personal information including personal health information.(179)

10.1.4 The Social and Health Data Permit Authority

Findata is located at the Finnish Institute for Health and Welfare and is separate from the institute's other activities. It began operating officially in November 2019. The Ministry of Social Affairs and Health has appointed a steering group for the launch of the activities of the data permit authority for the secondary use of health and social sector data and to develop the services provided by the authority.(180) In the interim, data permit applications and information requests must be submitted to the respective data owners. From April 2020 onwards, Findata will grant permits for the secondary use of data stored in national registries and data saved in both public and private healthcare services. Permits for all data saved in the Kanta services will be granted from January 2021 onwards. Permits will be granted for a number of purposes as stipulated by the Act on the Secondary Use of Health and Social Data (552/2019).(181)

10.2 Legislation

Important legislation in place in Finland in relation to the collection, use and sharing of personal health information includes:

- The Act on handling Customer Data in Health and Social Care (159/2007)
- The Data Protection Act (1050/2018) (Tietosuojalaki)
- The Act on Electronic Prescription (61/2007)
- The Act on Secondary Use of Health and Social data (552/2019)

Legislation	Description
The Act on the Handling Customer Data in Health and Social Care	Under the Act on Handling Customer Data in Health and Social Care, public healthcare organisations are obliged to enter patient records in a nationally centralised archive. The aim of the Act is to strengthen the data security of processing patient information and patients' access to information. Private healthcare organisations that have an electronic system for long-term storage of patient records must comply with this legislation.(18)
The Data Protection Act (Tietosuojalaki)	Finland has passed a supplementary implementation act of the GDPR, the Data Protection Act of Finland (Tietosuojalaki), which came into force on 1 January 2018. The act complements the GDPR and repeals the Personal Data Act of 1999. In Finland, the Office of the Data Protection Ombudsman (Tietosuojavaltuutetun toimisto) is the local supervisory authority and has a number of roles and responsibilities under the Data Protection Act e.g. audits, right to receive information and right to impose sanctions on entities. The Finnish Data Protection Board was the decision-maker under the previous Personal Data Act 1999 and has since been disbanded.(182)
The Act on Electronic Prescription	The Act on Electronic Prescriptions provides that introduction of electronic prescriptions is mandatory for pharmacies, healthcare units, and self-employed persons with practices in healthcare units' premises. All prescriptions must be issued electronically. Telephone or paper prescriptions may be issued only in exceptional cases. The pharmacy will also convert

	these prescriptions into electronic form and record them in the Prescription Centre. The aims of the Act on Electronic Prescriptions are to improve patient and drug safety and to make prescribing and dispensing of medicines easier and more efficient. Patients have the right, by law, to[183]: ▪ check what details are stored about them ▪ examine the electronic prescription details in the Prescription Centre and Prescription Archive ▪ know who has handled their details stored in the Prescription Centre and Prescription Archive ▪ correct incorrect personal details.
The Act on Secondary Use of Health and Social data 2019	In May 2019, a law was laid down on the secondary use of health and social data. The purpose of the Act is to facilitate the effective and safe processing and access to the personal social and health data for steering, supervision, research, statistics and development in the health and social sector. A second objective is to guarantee an individual's legitimate expectations as well as their rights and freedoms when processing personal data. The secondary uses referred to in the Act include: ▪ scientific research ▪ statistics ▪ development and innovation activities ▪ steering and supervision of authorities ▪ planning and reporting duties by authorities ▪ teaching ▪ knowledge management.[184] The Act eliminates overlapping administrative burden related to the processing of permits, speeds up permit processing and ensures the smoother collation of data from different registers. The Social and Health Data Permit Authority role is described in Section 10.1.5.[185]

10.3 Consent model

10.3.1 Individual care

According to Kanta website (www.kanta.fi), a patient does not have a right to forbid storing their EHRs in the national patient data repository after the healthcare unit in question has started using the repository. Health data may not be shared without a written consent of the patient. Moreover, sharing of EHRs between healthcare service providers connected to the national data system services is subject to patient's consent (subject to certain exceptions). Once the consent is given, the consent covers all EHRs in the national data repository. The patient may, however, prohibit sharing of specific EHRs as determined by the patient. The consent (as well as any prohibitions) is given by a document signed by the patient or via an electronic portal (Omakanta).(186)

The primary use of an individual's data means that data is used for the purpose for which the data was originally saved for in the patient register.(185) Implied consent is used for the collection and primary use of patient data. Under the Act on Handling Customer Data in Health and Social Care, public healthcare organisations are obliged to enter patient records in a nationally centralised archive. Before the patient begins using the online national Kanta services in Finland, it will be explained to them what the Kanta services are and how their information will be used. This information will be given to the patient in healthcare units or they can acknowledge receipt of it online in My Kanta Pages.

Information about a patient's healthcare, medical care in particular, and test results are recorded in the Patient Data Repository (PDR). Patient data in the PDR can be used by the healthcare provider that recorded the data. A patient can limit the use of their data by restricting access to data (issuing a refusal); this can be done in the healthcare services or online in My Kanta Pages.(187)

Professionals browsing the data in the Patient Data Repository always require a care relationship with the personal data they view. Furthermore, medical records can only be accessed by healthcare employees who have a healthcare professional card. This means that only healthcare professionals involved in the direct care of a patient can view that patient's health information and they must have the authority to do so.

The Patient Data Repository log and control services help to ensure that patient records are used in compliance with data security and legislation. Access logs of the healthcare professionals and citizens accessing the systems are recorded.(188) Such measures ensure that the activity log tracks each person who has viewed individual health records and these logs are subject to audits.

10.3.2 Uses beyond the care of the individual

The Secondary Use of Health and Social Data Act 2019 allows for information created during health and social service sector activities to be used for purposes other than the primary reason for which it was originally collected and recorded.[21] The secondary use of individuals' data refers to the use of the same information in other contexts than in primary use. The secondary uses outlined in the Act include scientific research, compiling of statistics, development and innovation activities, teaching, knowledge management, steering and supervision of authorities, and the planning and reporting duties of authorities. Different provisions apply to the different uses of data. Only aggregate data from which individuals cannot be identified may be used in the development and innovation activities.[185]

Currently, research and collection of health information based on register data are carried out without separate consent from the individual by submitting permit applications to data controllers. In the future, this practice will continue, but in a more streamlined way. As discussed in Section 10.1.4, the Data Permit Authority, which will be in operation by 2020, will issue permits for all data saved in the Kanta services, eliminating the need for researchers and service providers to submit permit applications to multiple data controllers for access to registry data. The data permit authority will only supply the minimum amount of data necessary in each case, and all identifiers will be removed from the data.

The Secondary Use of Health and Social Data Act 2019 includes provisions on the data permit authority, its duties, and the secondary use of health and social data. A data permit authority grants data permits when data is needed from numerous different controllers or when data is saved in the Kanta service and or the data in question is register data from private social welfare and healthcare service providers. It does this by[21]:

- always supplying data in a manner that maximises the protection of personal data in each situation
- only supplying the minimum amount of data that is necessary for the instance in question
- collecting data saved by the various controllers, combining these and supplying them to the applicant for use in a secure user environment.

Free public access is only provided to aggregate data. All personal data is always processed in a secure user environment.

The Act on Finnish Institute for Health and Welfare allows for information created during health and social care service sector activities to be collected to national registries. These registries are further used to create national statistics and for monitoring, assessment and supervision of health and social care providers.

Collection of data to the registries is based on the law and does not require explicit consent.

10.4 eHealth developments

There are a number of ehealth initiatives in use in Finland, including:

- national health identifier
- Kanta Services (national data repository, electronic health records, patient portal, prescription services and pharmaceutical database).

10.4.1 National health identifier

Finnish personal identity codes were introduced in 1963. To use eHealth services such as online My Kanta Pages, patients need a Finnish personal ID code and means of identification such as online bank IDs, mobile IDs or an electronic identity card.[52,189,190]

10.4.2 Kanta Services

Finland is one of the first countries in the world to set up a national digital patient data repository covering both the public and private healthcare sectors. Public healthcare service providers are obliged to enter patient records in a nationally centralised archive. Private healthcare service providers are obliged to join the national data system services if the long-term storage of their health records is carried out electronically.

Kanta produces a number of digital services for the social welfare and healthcare sector, including[188]:

- **My Kanta Pages —** This is a service that records health information about the patient including clinical history and prescriptions. It can be used by patients to access their healthcare information online and register declarations such as consent.
- **Prescription service —** All prescriptions are issued electronically. Paper or telephone prescriptions can be issued only in exceptional cases. All prescriptions are issued and dispensed via the Kanta services.
- **Pharmaceutical Database —** A database that contains necessary information about medicines, their price and reimbursement status etc. Information about individual products can be looked up in the Medicinal Products Database.
- **Patient Data Repository —** Patient documents and patient information are stored in electronic format in Finland in the Patient Data Repository.

10.4.3 Electronic Health Records (EHR)

Kanta as such is not an EHR system but a data transmission and archiving service. Kanta does not replace regional EHR systems, but healthcare units joining Kanta services must ensure interoperability of their EHR system with Kanta services.(186)

All patient documents are stored in electronic format in Finland. Healthcare professionals record the patient data in their local EHR solutions and then local EHR's transmit these data encrypted in an internationally standardised format to the national centralised integrated shared Kanta services, such as Patient Data Repository. The Patient Data Repository allows the centralised electronic archiving of patient records and long-term permanent storage of the data. The Patient Data Repository plays a central role in passing information between healthcare service providers. Patients can see the data recorded by the healthcare units via the online My Kanta Pages, as described in Section 10.4.2.

Kanta services records that a patient has been informed about eHealth services and contains records of a patients consent to disclose information and possible refusals of disclosure, together with cancellations of consents and refusals. It also holds information that is important for the patient's care, such as a living will or the patient's wishes regarding organ donation for another person. Through the service, healthcare units have access to the patient's main health information in one central repository.

10.4.4 ePrescription

In Finland, all medical prescriptions are electronic since 2017. Information on ePrescription is recorded in the Prescription Centre database, which is part of the Kanta services. When a patient is dealing with matters related to ePrescriptions, their oral consent is sufficient. Patients' written consent is only required in the event that a healthcare unit wishes to retrieve information from the Prescription Centre for a purpose other than the treatment they are getting.(191)

The patient can view their prescription information and renew an ePrescription through:

- My Kanta service
- their own healthcare provider
- a community pharmacy.

The patient can collect medication prescribed to them at any community pharmacy by:

- presenting a patient guide (information on the medicine as well as dosing instructions) provided by their doctor
- using their Kela card (a personal health insurance card)

- using their personal identification.

If consent to sharing prescription records is limited or refused by the patient, the records cannot be seen anywhere else but in the unit where the information has been recorded. If the patient refuses to share prescription data, community pharmacies and healthcare units cannot see the information on the prescription. However, the person who has prescribed the medicine is always able to view the prescriptions they have issued. All prescriptions are issued electronically and so paper or telephone prescriptions are only issued in exceptional cases. In cases of paper or telephone prescriptions, it is the legal duty of the community pharmacies to record these into the Prescription Centre.

If someone else is acting on behalf of a patient (for example, collecting a prescription from the pharmacy on a person's behalf) they must show the patient's instruction sheet of the prescription or the person's Kela card. When using a Kela card, the person acting on behalf of the patient must know which medicines they are collecting. It is also possible for the patient to give an e-authorisation to the person who is collecting their prescription medicines. When using e-authorisation, the person collecting the prescription medicines must know the personal identity code of the patient.(192)

Finland and Estonia have already established cross-border eHealth service collaboration for ePrescribing. Estonia and Finland have developed, along other European Union member states, common interoperable cross-border health information exchange data systems. Finnish patients are the first in Europe who can go to a community pharmacy in Estonia and collect their medication, with some restrictions, which was prescribed electronically by their physician in Finland. The initiative applies to all ePrescriptions prescribed in Finland, provided consent has been given and the Estonian community pharmacies have signed the agreement. (193) The Finnish ePrescriptions can be used also in Croatia.

10.5 Patient engagement

In 2018, Finland launched a 'data is good' campaign by using examples of the benefits of healthcare data. The campaign ran for 100 days and focused on publishing the benefits of health data. Examples of benefits are given below:

Benefits to the patient:

- Register research helps to access the health and well-being of the Finnish population, for example, incidence of cardiovascular disease
- By taking part in health surveys, you are contributing to the information landscape and this helps decision makers to plan services that meet patient needs
- Health surveys help determine the most appropriate health initiative that are best suited to Finns
- Statistics allow researchers to create better treatment and medications for patients and for future generations
- New innovative information technology applications can be developed when developers have access to the health information of the population.

Benefits for health and social care professionals:

- High-quality information allows for informed decision making and leads to a high level of care
- Information healthcare professionals provides can impact on how their healthcare institute appears in national statistic and assists in clinical audits
- Having access to comparable health information that is of good quality can help identify outliers in local health regions
- Good quality data can help control and monitor disease
- Data is used to support national, regional and local decision-making, ensuring services are working efficiently.

10.6 Key learnings

- Finland has a national health identifier, national electronic health records, ePrescription and an online accessible patient portal (My Kanta Pages).
- Consent is not needed for the collection of personal health information as public healthcare organisations are obliged to enter patient records in a nationally centralised integrated and shared repositories.
- Implied consent is used in the provision of individual care within the healthcare provider a patient attends.
- Explicit consent is needed if information is shared with external healthcare providers. Patients can give consent at point of care or online through My Kanta Pages.
- Secondary use of personal health information is allowed if a permit has been issued by the Health and Social Data Permit Authority (Findata).
- Health information should always pseudonymised or anonymised when shared for research or planning purposes unless a permit has been granted from the data permit authority.
- Finland is one of the first countries in the world to set up a comprehensive national electronic patient data repository and client data repository for social welfare services.
- Having one electronic set of services, the Kanta services, means that any national infrastructure is required to be interoperable with Kanta. Since Kanta also provides for other e-Health solutions such as ePrescription, interoperability with these systems is ensured through this national interface.

11. Denmark

Denmark has a population of 5.7 million people.[194] The Danish healthcare system is universal and based on the principles of free and equal access to healthcare for all citizens. The healthcare system offers high-quality services, the majority of which are financed by general taxes. The healthcare system operates across three political and administrative levels: the state, the regions and the municipalities.[194] The state holds the overall regulatory and supervisory functions in health and elderly care. The five regions are primarily responsible for the hospitals, the general practitioners (GPs) and psychiatric care. The 98 municipalities are responsible for a number of primary healthcare services as well as for elderly care.

eHealth at a glance:

- All GPs keep electronic health records (EHRs). Information from these EHRs then gets added to national health registries
- ePrescribing — 99% of all prescriptions are sent electronically to the pharmacies
- eReferral — 97% of all referrals to hospitals are made electronically
- Shared Medication Record — contains up-to-date information on every citizen in Denmark and is shared across all local systems in healthcare
- Patient portal — Sundhed.dk allows citizens to access their own medical data from national health registers, EHRs and medication data.

Consent model overview:

- Consent is implied for the provision of direct care. By accepting treatment, the patient accepts that their health information will be shared for the purpose of their treatment.
- EHRs are created without the consent of the individual.
- Legislation in Denmark allows for health information to be used for secondary purposes, without consent of the individual, providing that:
  - approval is granted from an authorised authority
  - that the information is necessary for statistical or scientific studies of significant public importance and that the processing is necessary for carrying out these studies.
- Electronic records can only be accessed by healthcare professionals involved in their patient's direct care. The use of access logs creates transparency and contributes to a high level of public trust in eHealth initiatives in Denmark.

11.1 Key organisations

There are a number of key organisations with varying responsibilities in relation to personal health data (collection, use and sharing) in Denmark, including:

- the Ministry of Health
- Danish Health Data Authority
- Danish Data Protection Agency (Datatilsynet)
- Danish Quality Improvement Programme (RKKP)
- MedCom (project organisations that run cross sectorial IT projects and solutions)
- Sundhed.dk (national eHealth portal).

11.1.1 The Ministry of Health

The Ministry of Health consists of a department as well as a number of boards and authorities that work to ensure a well-functioning and efficient health system. Some of the ministry's organisations are listed below:

- Danish Health Authority
- Danish Medicines Agency
- Danish Patient Safety Agency
- Danish Patient Complaints Board
- Danish Health Data Authority
- State Serum Institute (National centre of disease control)
- National Science Ethics Committee
- Ethical Council
- National Genome Centre.[195]

11.1.1.1 Danish Health Data Authority

The main task of the Health Data Authority is to support the health field by collecting and providing health information to health professionals as well as to policy makers and citizens. They create coherent data and digital solutions for the benefit of citizens, patients and healthcare professionals as well as for management, statistical and scientific purposes in the health and elderly sectors. The Health Data Authority is part of the Danish Ministry of Health and is responsible for a large number of databases, registers, services and infrastructure that involve data on diagnosis, treatment (including drug prescriptions) and population health.[196] The information in the registers comes from hospitals and general practitioners who record every time a person has been in contact with the Danish healthcare system. There are a number of registries such as the National Children's Database, the National Patient Registry, the Product Statistics Register and the Death Register. The Danish Health Data Authority publishes a large number of reports based on data from the health registers. The figures provided in these reports provide a comprehensive overview of the health of the population. The Danish Data Protection Agency oversees that the

legal requirements concerning healthcare data are satisfied before data are used in research projects or clinical trials.(194)

11.1.2 Danish Data Protection Agency (Datatilsynet)

The Danish Data Protection Agency (Datatilsynet) is the administrative authority assigned with the task to ensure compliance with the Act on Processing of Personal Data, now superseded by the General Data Protection Regulation and the Danish Data Protection Act (databeskyttelsesloven).(197)

11.1.3 Danish Quality Improvement Programme

The Danish Healthcare Quality Programme is a national system intended to support continuous quality improvement of the Danish healthcare service as a whole. It generates methods to persistently develop quality across the entire healthcare sector in Denmark; providing standards for good quality and developing methods to measure and control this quality.(198)

11.1.4 MedCom

MedCom was established in 1994 as a public funded, non-profit cooperation. MedCom facilitates the communication between authorities, organisations and private firms linked to the Danish healthcare sector. MedCom is financed and owned by the Ministry of Health, Danish Regions and Local Government Denmark. It has four main activities:

- Cross-sector dissemination — providing support and information for healthcare professionals, particularly through telemedicine solutions and exchange of data such as exchanges of journals and electronic referrals.
- Standard, test and certification — MedCom's standards are the foundation for exchanges of relevant data between the different parts of the healthcare sector. MedCom documents, tests and certifies IT vendors' implementation as well as offering support, consultancy and training courses.
- System management — MedCom is responsible for a number of public IT solutions.
- Application, participation and project-management in relation to EU projects are part of MedCom's international activities. In addition, MedCom promotes Danish health IT and international standardisation initiatives.(199)

11.1.5 Sundhed.dk

Sundhed.dk is the national eHealth portal in Denmark. Since its launch in 2003, sundhed.dk provides several functionalities such as quality assured health information, access to some parts of medical records and medication, and an overview of the Danish healthcare system. It allows the public to access some parts of their health records (hospital records, medication records and any other interaction with the healthcare services in Denmark) in one location. Health professionals can also log on and gain secure and controlled access to personal data regarding patients they are actively treating. Around 1.3 million patients access sundhed.dk each month.[200]

11.2 Legislation

Important legislation in place in Denmark in relation to the collection, use and sharing of personal health information includes:

- The Act on Processing of Personal Data (Persondataloven)
- The Danish Act of Health (Sundhedloven)
- The Ministry of Health and the Elderly's Data Protection policy
- Act on Research Ethics Review of Health Research Projects (no. 593, 14 June 2011).

Legislation	Description
The Act on Processing of Personal Data (Persondataloven)	The EU's General Data Protection Regulation (GDPR) and the Danish Data Protection Act (databeskyttelsesloven) replace the Danish Personal Data Act (persondataloven) and give certain rights to individuals. Principles for collecting personal data are set out under the General Data Protection Regulation and are further supported by the individual implementation of legislation on data protection in each country within the General Data Protection Regulations framework. Personal data can only be collected for lawful purposes and the amount of personal data collected is limited to what is necessary to fulfill that specific purpose.[201]
The Danish Act of Health (Sundhedloven)	The Health Act encompasses all legislation on benefits pertaining to public healthcare, including mental healthcare and patient's rights.[202] In May 2014, the Executive Order for the Shared Medication Record (FMK — Fælles Medicinkort) was adopted under the Health Act. The Executive Order describes in detail which professional groups and groups of persons who are permitted access to FMK as well as the rights and obligations associated with the individual professional groups.[203]
The Ministry of Health and the Elderly's Data Protection policy	The Ministry of Health and Elderly's data protection policy provides information on how the Ministry and its institutions collect, handle and protect personal information. When an institution collects personal information directly from citizens, that institution must inform the individual of the purpose of the data processing, the time period for the retention of personal data and the person's individual rights as the data subject.[195]
Act on Research Ethics Review of Health Research Projects (no. 593, 14 June 2011)	The Act on Research Ethics Review of Health Research Projects lays down the legal framework used by ethical review committees to evaluate research projects regarding biological material or data obtained when making a genetic analysis. For the purposes of ethical review there is one national research ethics committee and 11 regional committees. The Danish National Committee on Health Research Ethics coordinates the work of regional committees.[204]

11.3 Consent model

11.3.1 Individual care

According to the Danish Health Act, consent is implied for direct care; by accepting treatment the patient is accepting that their personal health information will be shared for the purpose of their treatment. Registering a patient's health information is a prerequisite for healthcare professionals to be able to deliver high quality care. Similarly, healthcare professionals must have access to the relevant information when providing care to a patient. Health professionals can retrieve the information in their 'local journal' (local GP/hospital electronic record), but they can also, when appropriate and necessary, 'retrieve data from outside'.(205) In Denmark, primary processing of health data is governed by the Health Act (Sundhedsloven no. 1202, 14 November 2014), the Danish Data Protection Act (databeskyttelsesloven), the EU's General Data Protection Regulation (GDPR) and the Act on Research Ethics Review of Health Research Projects (no. 593, 14 June 2011).(204)

11.3.2 Uses beyond the care of the individual

As a general rule, public authorities, including the institutions of the Ministry of Health and the Elderly, process personal data under the Act on Processing of Personal Data. This means that data processing does not require consent of the individual. Secondary use of health data by other organisations requires the approval of an authority, depending on where the data is derived from, for example, a register or a medical journal. Data controller and the data processor must keep an internal register of the data processing. In practice, this means that the use of national population-based health data registers from the Danish Health Data Authority is contingent on the research project satisfying the requirements set out in the data protection law as being of significant public importance and that the processing is necessary for carrying out the studies.(206)

11.3.3 Research

Secondary use of health-related data is regulated in Denmark partly by the by the Research Ethics Review of Health Research Projects and Health Act (Sundhedsloven no. 1202, 14 November 2014) the Danish Data Protection Act (databeskyttelsesloven), and the EU's General Data Protection Regulation (GDPR). The general rule under the the Danish Data Protection Act (databeskyttelsesloven), the EU's General Data Protection Regulation (GDPR) relating to the processing of already existing health data and other sensitive data for research purposes is that they may be processed without consent of the data subject presupposing that the processing is carried out for:

- statistical or scientific studies of significant public importance and the processing is necessary for carrying out these studies.

- approval from an authority — depending on where the data is derived from, for example, a register or a medical journal.

A list of all health related registries, a description of each registry and details of primary variables used in the registry, can be found on the National Centre for Register-based Research website.(207) Information used for statistical analysis or research purposes can often include personal information such as gender and age. Data sets that are available for statistical purposes and research purposes are provided at aggregated level and are pseudonymised. This means that the identifiable information such as CPR-number (personal identification number) is replaced by an ID number so that the person cannot be immediately identified.(208) Researchers can obtain access to these data, either in a safe environment on the Research Machine (Forskermaskinen) or by ordering data extractions. The data extractions are delivered in a secure environment and made available to the researcher. When applying for data, researchers must meet a number of requirements; a project description and an extension description must be attached, containing information about which registries, variables, population and period that apply to the project.(209)

11.3.4 Safeguarding personal health information

The Data Inspectorate and the National Audit Office regularly monitor the Danish Health and Medicines Authority practices, ensuring that the organisation is safeguarding personal health information and using it appropriately. The recommendations that follow from inspections are incorporated into the work plans of the authority, thereby promoting continuous improvement in safety.(204)

11.4 eHealth developments

There are a number of eHealth initiatives in use in Denmark, including:

- national health identifiers
- electronic health records
- Sundhed.dk web portal
- Shared Medication Record.

11.4.1 National health identifiers

Unique patient identifiers are used across health and social care and civil administration databases.(210)

11.4.1 Electronic Health Records (EHR)

All GPs keep electronic health records (EHRs), and 98 per cent exchange records electronically. In general, the Danish healthcare legislation perceives creation of health records and making use of health data primarily as a matter of quality assurance and patient safety. Licensed healthcare professionals are under an

obligation to keep records, and non-compliance can lead to disciplinary sanction (and in severe cases even to withdrawal of license).[202] Every time patients in Denmark attend the doctor, the pharmacy, the emergency room or have any other contact with the healthcare system, the healthcare professional records information about the event in the patients electronic record. This data is added to national registries such as the National Patient Register (Lands Patient Register), which is managed by the Danish Health Data Authority. These health registries provide an overview of the activities in the healthcare system and the Danes' state of health.[194]

11.4.2 Sundhed.dk web portal

The web portal Sundhed.dk allows citizens to access their own medical data such as EHRs at hospitals, medication data and laboratory results. These data can also be accessed by the patient's GP. Patients can also access general information on health, diseases and patient rights through this online portal.[194]

11.4.3 Shared Medication Record

In 2007, the Danish Health Data Authority set out to establish a nationwide Shared Medication Record, containing up-to-date information on prescription medicine on every citizen in Denmark and shared across all local systems in the healthcare sector. 99% of all prescriptions are sent electronically to pharmacies.[194] With the shared involvement of many different stakeholders, including the Ministry of Health, the Danish Health Authority and local governments, a private vendor, together with the Danish Health Data Authority, developed the Shared Medical Record.[196] The Shared Medication Record (Fælles Medicinkort FMK in Danish) is a vital database at the Danish Health Data Authority, storing data on all Danish citizens' current medication plans, electronic prescriptions and medicine purchases. The Shared Medication Record has processed over 500 million prescriptions since it launched in 2009. The Shared Medication Record is used today by almost all healthcare professionals in Denmark across the sectors. In total, about 40 different systems have integrated with the Shared Medication Record. Patients can assess information about current prescriptions and prescriptions used in the last two years online using their NemID (common secure login used for banking/public services) via sundhed.dk or the FMK (Fælles Medicinkort) website. In addition to patients having access to their own data, healthcare professional involved in the patients care (doctors, dentists, nurses) can also access this information if the information is relevant to their treatment. Amendments made to the Health Act in 2010 specify which professional groups can access FMK and when they can access FMK. Information about who accesses is logged and review logs can be assessed by patients.[203]

11.4.5 eReferral

97% of all referrals to hospitals are made electronically.[194] All referrals to medical specialists and psychologists are made electronically.[194]

11.4.6 Strategy for use of healthcare data

Denmark is a world leader in unique healthcare registers and infrastructure for linking data across registers and databases. Biobanks and registers provide detailed information on the entire population that can be used for research and improvement of healthcare services. A reform to improve the visibility of results has been initiated and marks a commitment to a national long-term strategy for better use of healthcare data and for creating greater transparency of health outcomes and results. As part of the visibility of results reform, a Health Data Programme was established in 2014 to run over a four-year period. The vision of the Health Data Programme is to create 'better healthcare through better use of data', and four separate programme tracks have been defined to support this vision:

- New data model and user interface. Developing a modernised data model and easy accessible user interface that gives better access to relevant healthcare data for healthcare professionals, researchers, administrators and citizens.
- Modernised infrastructure. Developing the IT infrastructure for national health data management at the National Health Data Authority, including a modernised data platform.
- Better data quality. Enhancing quality of the healthcare data by establishing a new national governance model for monitoring data quality in order to support higher validity and reliability of healthcare data.
- Better cross-sectorial cooperation. A new governance model for health data management to support cross-sectorial cooperation.[194]

11.5 Patient engagement

11.5.1 Building a culture of trust

Sundhed.dk (the online eHealth portal) is one of the major accomplishments of Denmark's eHealth journey to date.

Denmark has a strong culture of trust, which is a key factor to the success of many eHealth initiatives. Trust in the health service and governing bodies has enabled the successful implementation of initiatives such as the patient portal. Denmark has worked to ensure that the public experience the advantages of data exchange and transparency, thus instilling confidence in the public that their data is safe.[152]

11.6 Key learnings

- Denmark has national health identifiers, electronic health records, ePrescribing, eReferral and a patient portal.
- All GPs keep EHRs. Information from these EHRs then gets added to national health registries. EHRs are created without the consent of the individual.
- Consent is implied for the provision of direct care. By accepting treatment, the patient accepts that their health information will be shared for the purpose of their treatment.
- Legislation in Denmark allows for health information to be used for secondary purposes, without consent of the individual, providing that:
  - approval is granted from an authorised authority
  - the information is necessary for statistical or scientific studies of significant public importance and that the processing is necessary for carrying out these studies.
- Electronic records can only be accessed by healthcare professionals involved in their patient's direct care. The use of access logs creates transparency and contributes to a high level of public trust in eHealth initiatives in Denmark.

Appendix 1: Key terms in relation to health information and how it is used

Individual care — The use of a person's health information for their own diagnosis, care and treatment by health and social care professionals. This is also known as primary use of health information, or the use of information for direct care.

Secondary use of health information — The use of a person's health information for purposes beyond their own diagnosis, care and treatment. The two main types of secondary use are:

- service planning
- research.

As the term secondary use is quite technical, it is recommended that when engaging with patients and the public the following term is used instead: the use of health information beyond the care of the individual.

Personally identifiable — Details from patient records that can be linked to a specific person because they include, date of birth, postcode or any other piece of information that identifies the person. This information should be stored in a highly secure way.

De-personalised — Health information that cannot easily be linked to a specific person because any piece of information that identifies the individual has been removed, disguised or encrypted. Although this information cannot easily be linked back to the patient, with enough time and the right resources, the person could be identified.

Anonymous — Health information from many people that has been combined together to show general trends and therefore could not be linked to a specific person. As it only relates to large groups of people, it cannot be linked back to a single person, and so it has fewer security measures attached to it.

Appendix 2: Key terms in relation to consent

Explicit consent — A requirement that an individual signifies his or her agreement with a data controller by some active communication between the parties.

Implied consent — Implied consent arises where consent may reasonably be inferred from the action or inaction of the individual.

Informed consent — Detailed information given to the individual along with opportunity for discussion. The individual then provides clear and affirmative action to allow data to be collected and used.

Opt-in — Person has to actively sign-up for data to be collected and used.

Opt-out — Data will be collected and used automatically unless person actively dissents.

Appendix 3: Key terms in relation to eHealth

eHealth or electronic health — This is defined by the World Health Organisation as the use of information and communication technologies for health.

National electronic health record — A digital record of a patient's journey through healthcare.

Shared care record — A record that enables healthcare providers in different settings (for example, primary care or hospitals) to view patient records with the patient'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.

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

Individual health identifier — A unique number given to a patient which allows them to be identified across healthcare organisations.

Patient portal — A website specially created to be used by patients. Patients can log in securely and view their own health record information, sometimes at an individual healthcare organisation.

ePrescribing — The process of sending medical prescriptions from healthcare professionals – via a computerised system – to pharmacies.

eReferrals or electronic referrals — An electronic platform that enables the seamless transfer of patient information from a primary to a secondary treating practitioner's client management system.

References

1. *Health Act 2007*. Available from: http://www.irishstatutebook.ie/eli/2007/act/23/enacted/en/print. Accessed on: 14 May 2019.

2. Fiona Caldicott. *Information: To share or not to share. Information Governance Review*. 2013. Available from: http://collections.crest.ac.uk/9560/1/Information%20Governance%20Review.pdf. Accessed on: 07 March 2019.

3. Citizens Information. *Overview of the General Data Protection Regulation (GDPR)*. 2018. Available from: https://www.citizensinformation.ie/en/government_in_ireland/data_protection/overview_of_general_data_protection_regulation.html. Accessed on: 14 May 2019.

4. Department of Health. *eHealth Strategy for Ireland*. 2013. Available from: http://www.dohc.ie/publications/eHealth_Strategy_2013.html. Accessed on: 10 April 2019.

5. Health Service Executive. *Knowledge & Information Strategy*. 2015. Available from: http://www.ehealthireland.ie/Knowledge-Information-Plan/Knowledge-and-Information-Plan.pdf. Accessed on: 20 November 2018.

6. Department of Public Expenditure and Reform. *National Development Plan 2018-2027*. 2019. Available from: https://www.gov.ie/en/publication/83fec4-national-development-plan/. Accessed on: 14 May 2019.

7. Government of Ireland. *Sláintecare Implementation Strategy*. 2018. Available from: https://assets.gov.ie/9914/3b6c2faf7ba34bb1a0e854cfa3f9b5ea.pdf. Accessed on: 27 August 2018.

8. *Data Protection Act 2018*. Available from: http://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/print. Accessed on: 14 May 2019.

9. Data Protection Commission. *Background*. 2018. Available from: https://www.dataprotection.ie/en/about/background. Accessed on: 14 May 2019.

10. Health Research Board (HRB). *Data Protection Act 2018 (Section 36(2)) (Health Research) Regulations 2018*. 2018. Available from: https://www.hrb.ie/funding/gdpr-guidance-for-researchers/gdpr-and-health-research/health-research-regulations-2018/. Accessed on: 14 May 2019.

11. Citizens Information. *Controlling and processing data under GDPR - concepts and principles*. 2018. Available from: https://www.citizensinformation.ie/en/government_in_ireland/data_protection/controlling_and_processing_data_under_the_GDPR.html. Accessed on: 14 May 2019.

12. *Health Identifiers Act 2014*. Available from: http://www.irishstatutebook.ie/eli/2014/act/15/. Accessed on: 14 May 2019.

13. *Health (Provision of Information) Act, 1997*. Available from: http://www.irishstatutebook.ie/eli/1997/act/9/enacted/en/html. Accessed on: 14 May 2019.

14. Milieu LTD and Time.Lex. *Overview of the national laws on electronic health records in the EU Member States. National Report for Ireland*. 2013. Available from: https://ec.europa.eu/health/sites/health/files/ehealth/docs/laws_ireland_en.pdf. Accessed on: 14 May 2019.

15. Data Protection Commission. *What we do*. 2019. Available from: https://www.dataprotection.ie/en/about/what-we-do. Accessed on: 14 May 2019.

16. J Cassell J Stockdale, E Ford. *"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*. 2018. Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6402072/pdf/wellcomeopenres-3-16368.pdf. Accessed on: 19 March 2019.

17. Ontario Ministry of Health. *Ontario's Personal Health Information Privacy Legislation for the Health Sector (Health Sector Privacy Rules)*. Available from: http://www.health.gov.on.ca/en/common/ministry/publications/reports/phipa/phipa_mn.aspx. Accessed on: 24 October 2019.

18. Kanta. *Kanta privacy statements*. Available from: https://www.kanta.fi/en/privacy-statements. Accessed on: 1 May 2019.

19. Northern Ireland Department of Health. *Code of Practice on Protecting the Confidentiality of Service User Information*. 2019. Available from: https://www.health-ni.gov.uk/publications/code-practice-protecting-confidentiality-service-user-information. Accessed on: 10 August 2019.

20. Privacy Commissioner. *Health Information Privacy Code 1994*. Available from: https://www.privacy.org.nz/the-privacy-act-and-codes/codes-of-practice/health-information-privacy-code-1994/. Accessed on: 18 April 2019.

21. Government of Finland. *Secondary use of health and social data*. 2019. Available from: https://stm.fi/en/secondary-use-of-health-and-social-data. Accessed on: 24 October 2019.

22. Australian Government Department Of Health. *Framework to guide the secondary use of My Health Record system data*. 2018. Available from: http://www.health.gov.au/internet/main/publishing.nsf/content/F98C37D22E65A79BCA2582820006F1CF/$File/MHR_2nd_Use_Framework_2018_ACC_AW3.pdf. Accessed on: 10 April 2019.

23. Siggins Miller. *Evaluation of the Participation Trials for the My Health Record*. 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: 12 August 2019.

24. The Commonwealth Fund. *The English Health Care System.* Available from: https://international.commonwealthfund.org/countries/england/. Accessed on: 16 May 2019.

25. NHS England. *Data and Information*. Available from: https://www.england.nhs.uk/ourwork/tsd/data-info/. Accessed on: 28 August 2019.

26. NHS Digital. *Secondary Uses Service (SUS)*. 2019. Available from: https://digital.nhs.uk/about-nhs-digital/our-work/keeping-patient-data-safe/gdpr/gdpr-register/secondary-uses-service-sus-data-gdpr-information. Accessed on: 17 June 2019.

27. NHS Digital. *Spine*. 2019. Available from: https://digital.nhs.uk/services/spine. Accessed on: 28 August 2019.

28. Gov.uk. *Public Health England. About us*. 2019. Available from: https://www.gov.uk/government/organisations/public-health-england/about. Accessed on: 20 August 2019.

29. Government of the UK. *Health and Social Care (National Data Guardian) Act 2018*. 2018. Available from: https://www.legislation.gov.uk/ukpga/2018/31/contents/enacted. Accessed on: 28 August 2019.

30. National Data Guardian. *About us*. 2019. Available from: https://www.gov.uk/government/organisations/national-data-guardian/about. Accessed on: 27 August 2019.

31. National Data Guardian (UK). *Review of data security, consent and opt-outs*. 2016. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/535024/data-security-review.PDF. Accessed on: 26 Match 2019.

32. NHSX. *What we do*. 2018. Available from: https://www.nhsx.nhs.uk/what-we-do. Accessed on: 10 December 2019.

33. Data and technology in health and care The future of healthcare: our vision for digital. 2018. Available from: https://www.gov.uk/government/publications/the-future-of-healthcare-our-vision-for-digital-data-and-technology-in-health-and-care/the-future-of-healthcare-our-vision-for-digital-data-and-technology-in-health-and-care. Accessed on: 14 April 2019.

34. NHS. *NHS Long Term Plan*. 2020. Available from: https://www.longtermplan.nhs.uk/. Accessed on: 10 January 2020.

35. Information Commissioners Office (UK). *Guidance on consent*. 2018. Available

from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/. Accessed on: 03 April 2019.

36. Information Commissioners Office (ICO). *Data Sharing Code of Practice*. 2011. Available from: https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf. Accessed on: 13 June 2019.

37. Information Commissioners Office (ICO). *Anonymisation: managing data protection risk code of practice*. 2012. Available from: https://ico.org.uk/media/1061/anonymisation-code.pdf. Accessed on: 13 June 2019.

38. Government of the UK. *Health and Social Care (Safety and Quality) Act 2015*. 2015. Available from: https://www.legislation.gov.uk/ukpga/2015/28/contents/enacted. Accessed on: 28 August 2019.

39. NHS Digital. *Information Sharing Resources*. 2019. Available from: https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/information-governance-alliance-iga/information-governance-resources/information-sharing-resources. Accessed on: 28 March 2019.

40. Government of the Uk. *The Health Service (Control of Patient Information) Regulations 2002*. 2002. Available from: https://www.legislation.gov.uk/uksi/2002/1438/contents/made. Accessed on: 24 September 2019.

41. Government of the UK. *Access to Health Records Act 1990* 1990. Available from: https://www.legislation.gov.uk/ukpga/1990/23/contents. Accessed on: 28 August 2019.

42. Government of the Uk. *Access to Medical Reports Act 1988* 1988. Available from: https://www.legislation.gov.uk/ukpga/1988/28/contents. Accessed on: 28 August 2019.

43. Government of the UK. *Data Protection Act 2018*. 2018. Available from: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted. Accessed on: 28 August 2019.

44. European Commission. *REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).* . 2016. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN. Accessed on: 11 March 2019.

45. Gov.uk. *NHS Constitution for England* 2012. Available from: https://www.gov.uk/government/publications/the-nhs-constitution-for-england.

Accessed on: 13 June 2019.

46. Department of Health (UK). *Your Data: Better Security, Better Choice, Better Care*. 2017. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/627493/Your_data_better_security_better_choice_better_care_government_response.pdf. Accessed on: 3 April 2019.

47. NHS Digital. *National data opt-out programme*. 2019. Available from: https://digital.nhs.uk/services/national-data-opt-out-programme. Accessed on: 26 March 2019.

48. NHS Digital. *National Data Opt-out*. 2019. Available from: https://digital.nhs.uk/data-and-information/publications/statistical/national-data-opt-out/march-2019/ndop-mar19. Accessed on: 29 August 2019.

49. NHS Digital. *National data opt-out operational policy guidance document*. 2019. Available from: https://digital.nhs.uk/services/national-data-opt-out-programme/operational-policy-guidance-document. Accessed on: 5 August 2019.

50. NHS England. *England Scotland Wales Identifier* Available from: https://www.nhs.uk/using-the-nhs/about-the-nhs/what-is-an-nhs-number/#. Accessed on: 28 August 2019.

51. Health Information and Quality Authority (HIQA). *International Review of Unique Health Identifiers for Individuals*. 2010. Available from: https://www.hiqa.ie/sites/default/files/2017-02/International-Review-of-Unique-Health-Identifiers-for-Individuals.pdf. Accessed on: 11 March 2019.

52. eHealth-Era. *eHealth Strategies-Finland*. Available from: http://ehealth-strategies.eu/database/documents/Finland_eHealth-ERA_country_report.pdf Accessed on: 30 April 2019.

53. NHS Digital. *Summary Care Records (SCR)*. 2019. Available from: https://digital.nhs.uk/services/summary-care-records-scr. Accessed on: 3 April 2019.

54. NHS Digital. *Summary Care Records (SCR)*. 2019. Available from: https://digital.nhs.uk/services/summary-care-records-scr#using-scr. Accessed on: 7 January 2020.

55. NHS Digital. *Information Governance for Summary Care Records (SCR)*. 2019. Available from: https://digital.nhs.uk/services/summary-care-records-scr/information-governance-for-scr. Accessed on: 3 April 2019.

56. Understanding Patient Data. *Local health and care exemplars announced*. 2018. Available from: https://understandingpatientdata.org.uk/news/local-health-and-care-record-exemplars-announced. Accessed on: 21 August 2019.

57. Great North Care Record. *Opt out*. Available from: https://www.greatnorthcarerecord.org.uk/opt-out/. Accessed on: 24 August 2019.

58. NHS Digital. *Electronic Prescription Service* Available from: https://digital.nhs.uk/services/electronic-prescription-service. Accessed on: 15 July 2019.

59. The Pharmaceutical Journal Carolyn Wickware. *Paper prescriptions will be a rare sight by next year, says NHS Digital programme lead*. 2019. Available from: https://www.pharmaceutical-journal.com/news-and-analysis/news/paper-prescriptions-will-be-a-rare-sight-by-next-year-says-nhs-digital-programme-lead/20206832.article?firstPass=false. Accessed on: 27 August 2019.

60. NHS. *Start Using Electronic Prescriptions*. Available from: https://www.nhs.uk/using-the-nhs/nhs-services/pharmacies/electronic-prescription-service/. Accessed on: 24 September 2019.

61. NHS Digital. *NHS e-Referral Service*. 2019. Available from: https://digital.nhs.uk/services/e-referral-service. Accessed on: 29 August 2019.

62. Tjeerd-Pieter van Staa, Iain Buchan Ben Goldacre, Liam Smeeth. *Big health data: the need to earn public trust*. 2016. Available from: https://www.bmj.com/content/bmj/354/bmj.i3636.full.pdf. Accessed on: 29 September 2019.

63. Vojin Rakic Sigrid Sterckx, Julian Cockbain, Pascal Borry. *"You hoped we would sleep walk into accepting the collection of our data": controversies surrounding the UK care.data scheme and their wider relevance for biomedical research* [journal article]. 177-90]. 2016. Available from: https://doi.org/10.1007/s11019-015-9661-6. Accessed on: 19 April 2019.

64. Understanding Patient Data. *About us*. 2017. Available from: https://understandingpatientdata.org.uk/about-us. Accessed on: 21 August 2019.

65. Understanding Patient Data. *Evaluating Understanding Patient Data* 2018. Available from: https://understandingpatientdata.org.uk/sites/default/files/2018-12/UPD%20evalutation%20report%202018_2.pdf. Accessed on: 27 August 2019.

66. Curved Thinking. *Understanding public expectations of the use of health and care data*. 2019. Available from: https://understandingpatientdata.org.uk/sites/default/files/2019-07/Understanding%20public%20expectations%20of%20the%20use%20of%20health%20and%20care%20data.pdf. Accessed on: 27 August 2019.

67. Belfast Health and Social Care Trust. *Health Service Structure*. Available from: http://www.belfasttrust.hscni.net/about/Understanding-Health-Service-Structure.htm. Accessed on: 7 May 2019.

68. Northern Ireland Department of Health. *About the Department of Health* Available from: https://www.health-ni.gov.uk/about-department-health-social-services-and-public-safety#toc-3. Accessed on: 09 August 2018.

69. HSC. *About the programme*. Available from:

http://www.ehealthandcare.hscni.net/. Accessed on: 16 May 2019.

70. Information Comissioner's Office. *Information Commissioner Office Home*. Available from: https://ico.org.uk/. Accessed on: 23 April 2019.

71. Department of Health Northern Ireland. *Privacy Advisory Committee - Terms of Reference _July 2006)*. 2006. Available from: http://www.privacyadvisorycommittee.hscni.net/PAC%20Terms%20of%20Reference_July%202006.pdf. Accessed on: 9 September 2019.

72. Government of the UK. *Data Protection Act* 2018. Available from: https://www.legislation.gov.uk/ukpga/2018/12/schedule/15/crossheading/northern-ireland. Accessed on: 9 September 2019.

73. NI Direct. *Freedom of information and data protection*. Available from: https://www.nidirect.gov.uk/articles/freedom-information-and-data-protection. Accessed on: 23 April 2019.

74. Invest Northern Ireland. *Freedom of Information*. Available from: https://www.investni.com/about-us/freedom-of-information.html. Accessed on: 16 May 2019

75. Information Commissioners Office. *What are PECR?* Available from: https://ico.org.uk/for-organisations/guide-to-pecr/what-are-pecr/. Accessed on: 16 May 2019

76. Government Legislation. *Health and Social Care (Control of Data Processing) Act (Northern Ireland) 2016*. Available from: http://www.legislation.gov.uk/nia/2016/12/notes. Accessed on: 16 May 2019.

77. NHS England. *Northern Ireland*. Available from: https://www.datadictionary.nhs.uk/data_dictionary/attributes/h/health_and_care_number_de.asp?shownav=1?query=%22health+and+care+number%22&rank=100&shownav=1. Accessed on: 13 June 2019.

78. Personal Communication Mary McCluskey NIECR 10 April 2019.

79. Health Information and Quality Authority (HIQA). *ePrescribing: An international review*. 2018. Available from: https://www.hiqa.ie/sites/default/files/2018-05/ePrescribing-An-Intl-Review.pdf. Accessed on: 15 July 2019.

80. Health and Social Care Northern Ireland. NIECR Data Sharing Agreement. 2019.

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

82. Health and Social Care Northern Ireland. *Privacy Advisory Committee, Northern Ireland*. Available from: http://www.privacyadvisorycommittee.hscni.net/.

Accessed on: 09 September 2019.

83. Stats NZ. *Population clock*. 2019. Available from: http://archive.stats.govt.nz/tools_and_services/population_clock.aspx. Accessed on: 10 December 2019.

84. World Health Organization Ministry of Health New Zealand. *Health Service Delivery Profile 2012 (2012)* 2012. Available from: http://www.wpro.who.int/health_services/service_delivery_profile_new_zealand.pdf. Accessed on: 14 May 2019.

85. Ministry of Health. *eHealth*. 2019. Available from: https://www.health.govt.nz/our-work/ehealth. Accessed on: 18 April 2019.

86. New Zealand Ministry of Health. *Health Information Governance Guidelines*. 2017. Available from: https://www.health.govt.nz/publication/hiso-100642017-health-information-governance-guidelines. Accessed on: 10 September 2019.

87. Ministry of Health. *HISO 10029:2015 Health Information Security Framework*. 2015. Available from: https://www.health.govt.nz/publication/hiso-100292015-health-information-security-framework. Accessed on: 14 May 2019.

88. MidCentral District Health Board. *New Zealand NHI*. 2019. Available from: http://www.midcentraldhb.govt.nz/PatientsandVisitors/GeneralInformation/Pages/NHI.aspx# Accessed on: 14 April 2019.

89. Privacy Commissioner. *Privacy Commissioner's Office* Available from: https://www.privacy.org.nz/about-us/about-privacy/. Accessed on: 24 May 2019.

90. *Health Information Privacy Code 1994*. Available from: https://www.privacy.org.nz/the-privacy-act-and-codes/codes-of-practice/health-information-privacy-code-1994/. Accessed on: 18 April 2019.

91. Ministry of Health. *Certification of health care services*. 2018. Available from: https://www.health.govt.nz/our-work/regulation-health-and-disability-system/certification-health-care-services. Accessed on: 17 April 2019.

92. Government of New Zealand. *Government Chief Data Steward* Available from: https://www.data.govt.nz/about/government-chief-data-steward-gcds/. Accessed on: 10 December 2019.

93. Digital Government of New Zealand. *Government Chief Digital Officer*. Available from: https://www.digital.govt.nz/digital-government/leadership-and-governance/government-chief-digital-officer-gcdo. Accessed on: 10 December 2019.

94. New Zealand Privacy Commissioner. *Health Information Privacy Fact Sheet 3: Disclosure of health information - the basics* Available from: https://privacy.org.nz/news-and-publications/guidance-resources/health-information-privacy-fact-sheet-3-disclosure-of-health-information-the-basics/. Accessed on: 14 August 2019.

95. Government of New Zealand. *New Zealand Public Health and Disability Act 2000*. 2000. Available from: http://legislation.govt.nz/act/public/2000/0091/72.0/DLM80051.html. Accessed on: 17 July 2019.

96. Government of New Zealand. *Health (Retention of Health Information) Regulations 1996*. 1996. Available from: http://legislation.govt.nz/regulation/public/1996/0343/latest/DLM225616.html. Accessed on: 17 July 2019.

97. Government of New Zealand. *Oranga Tamariki Act 1989*. 2018. Available from: http://www.legislation.govt.nz/act/public/1989/0024/127.0/DLM147088.html. Accessed on: 1 October 2019.

98. *Family Violence Act 2018*. 2019. Available from: http://www.legislation.govt.nz/act/public/2018/0046/latest/whole.html. Accessed on: 1 October 2019.

99. New Zealand Ministry of Health *Information Sharing Guidance for Health Professionals*. 2019. Available from: https://www.health.govt.nz/system/files/documents/publications/health-professional-guidance-information-sharing-from-1-july-2019.pdf. Accessed on: 1 October 2019.

100. Parliamentary Counsel Office. *Health Act 1956*. 2017. Available from: http://www.legislation.govt.nz/act/public/1956/0065/118.0/DLM305840.html. Accessed on: 13 June 2019.

101. New Zealand Privacy commissioner. Health Information Privacy Act Sheet 2: Collection of health information Available from: https://privacy.org.nz/news-and-publications/guidance-resources/health-information-privacy-fact-sheet-2-collection-of-health-information/. Accessed on: 14 August 2019.

102. *Health information and data use – guidance*. 2018. Available from: https://ethics.health.govt.nz/guides-templates-forms-0/health-information-and-data-use-%E2%80%93-guidance Accessed on: 18 April 2019.

103. Shared Care Record New Zealand. *Shared Electronic Health Record*. 2019. Available from: http://sharedcarerecord.org.nz/. Accessed on: 16 July 2019.

104. Privacy Commissioner. *Electronic Shared Care Records Elements of Trust*. 2014. Available from: https://www.privacy.org.nz/assets/Files/Reports-to-ParlGovt/Electronic-Shared-Care-Records-Elements-of-Trust-report-1.pdf. Accessed on: 18 April 2019.

105. New Zealand Ministry of Health. *New Zealand ePrescription Service*. 2017. Available from: https://www.health.govt.nz/our-work/ehealth/other-ehealth-initiatives/emedicines/new-zealand-eprescription-service. Accessed on: 16 July 2019.

106. Health Informatics New Zealand (HiNZ). *National Health Information Platform*

replaces Electronic Health Record. 2019. Available from: https://www.hinz.org.nz/news/452553/National-Health-Information-Platform-replaces-Electronic-Health-Record.htm. Accessed on: 16 July 2019.

107. Data Futures Partnership. *A Path to Social Licence, Guidelines for Trusted Data Use*. 2017. Available from: https://1slo241vnt3j2dn45s1y90db-wpengine.netdna-ssl.com/wp-content/uploads/2019/08/Trusted-Data-Use_2017.pdf. Accessed on: 14 May 2019.

108. Social Investment Agency. *Data Protection and Use*. 2019. Available from: https://sia.govt.nz/how-we-can-help/data-protection-and-use/. Accessed on: 10 December 2019.

109. Social Investment Agency. *What you told us*. 2019. Available from: https://sia.govt.nz/publications/reports/what-you-told-us/. Accessed on: 10 December 2019.

110. Government of Canada. *Canada's Health Care System*. Available from: https://www.canada.ca/en/health-canada/services/health-care-system/reports-publications/health-care-system/canada.html. Accessed on: 24 October 2019.

111. Ontario.ca. *Health care in Ontario*. Available from: https://www.ontario.ca/page/health-care-ontario. Accessed on: 24 October 2019.

112. Canadian Institute for Health Information. *About CIHI*. Available from: https://www.cihi.ca/en/about-cihi. Accessed on: 14 May 2019.

113. Canadian Institute for Health Information. *CIHI's Annual Report 2017-2018.* Available from: https://www.cihi.ca/sites/default/files/document/cihi-annual-report-2017-2018-en.pdf. Accessed on: 14 May 2019.

114. Canadian Institute for Health Information. *CIHI's Privacy Program.* Available from: https://www.cihi.ca/en/about-cihi/privacy-and-security. Accessed on: 13 May 2019

115. Consent and Capacity Board. *About Us*. Available from: http://www.ccboard.on.ca/scripts/english/aboutus/index.asp. Accessed on: 25 April 2019.

116. Canada Health Infoway. *About* Available from: https://www.infoway-inforoute.ca/en/about-us. Accessed on: 24 October 2019.

117. College of Dieticians of Ontario. *Sharing Personal Health Information within the Circle of Care.* Available from: https://www.collegeofdietitians.org/resources/privacy-and-confidentiality/circle-of-care/sharinginfo.aspx. Accessed on: 15 May 2019.

118. Information and Privacy Commissioner of Ontario. *The Acts*. Available from: https://www.ipc.on.ca/about-us/the-acts/. Accessed on: 24 October 2019.

119. Information and Privacy Commissioner. *Your Health Privacy Rights in Ontario.* Available from: https://www.ipc.on.ca/health/your-health-privacy-rights-in-ontario/. Accessed on: 24 April 2019.

120. Office of the Privacy Commissioner of Canada. *PIPEDA in brief*. Available from: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/. Accessed on: 24 October 2019.

121. Officer of the Privacy Commissioner of Canada. *Provincial legislation deemed substantially similar to PIPEDA*. Available from: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/provincial-legislation-deemed-substantially-similar-to-pipeda/. Accessed on: 24 October 2109.

122. Psychiatric Patient Advocate Office. *Legislation*. Available from: https://www.sse.gov.on.ca/mohltc/ppao/en/Pages/OtherResources/Legislation.aspx?openMenu=smenu_OtherResources. Accessed on: 24 April 2019.

123. Information and Privacy Commissioner of Ontario. *Consent and your personal health information*. Available from: https://www.ipc.on.ca/health-individuals/consent-and-your-personal-health-information/. Accessed on: 24 October 2019.

124. Ontarion Ministry of Health. *Health Protection and Promotion Act, R.S.O. 1990, c. H.7*. Available from: https://www.ontario.ca/laws/statute/90h07. Accessed on: 24 October 2019.

125. College of Respiraotry Therapists of Ontario. *What Happens Within the "Circle of Care" – Stays Within the "Circle of Care".* Available from: https://www.crto.on.ca/members-blog/what-happens-within-the-circle-of-care-stays-within-the-circle-of-care/. Accessed on: 15 May 2019.

126. Information and Privacy Commissioner of Ontario. *Frequently Asked Questions Personal Health Information Protection Act*. 2015. Available from: https://www.ipc.on.ca/wp-content/uploads/2015/11/phipa-faq.pdf. Accessed on: 24 October 2019.

127. eHealth Ontario. *Accessing your EHR*. Available from: https://www.ehealthontario.on.ca/en/ehr/accessing-your-ehr. Accessed on: 24 October 2019.

128. Information and Privacy Commissioner of Ontario. *Lock-box Fact Sheet*. 2005. Available from: https://www.ipc.on.ca/wp-content/uploads/resources/fact-08-e.pdf. Accessed on: 17 July 2019.

129. Information & Privacy Commissioner of Ontario. *Dispelling the myths surrounding de-identification: Anonymization remains a strong tool for protecting privacy*. 2011. Available from: https://www.ipc.on.ca/wp-

content/uploads/2016/11/anonymization.pdf. Accessed on: 9 January 2020.

130. Information and Privacy Commissioner. *Health Cards and Health Numbers - The Personal Health Information Protection Act*. 2015. Available from: https://www.ipc.on.ca/wp-content/uploads/Resources/PHIPA-hfaq-cards-e.pdf. Accessed on: 19 August 2019.

131. eHealth Ontario. *Whats an EHR?* Available from: https://www.ehealthontario.on.ca/en/ehrs-explained. Accessed on: 24 April 2019.

132. eHealth Ontario. *Accessing your EHR*. Available from: https://www.ehealthontario.on.ca/en/ehr/accessing-your-ehr. Accessed on: 24 April 2019.

133. eHealth Ontario. *It's Working For You*. Available from: https://www.ehealthontario.on.ca/en/about-us/its-working-for-you. Accessed on: 13 May 2019

134. Pharmacy Connection. *Navigating Electronically Generated Prescriptions*. Available from: http://www.ocpinfo.com/library/practice-related/download/Navigating%20Electronically%20Generated%20Prescriptions.pdf. Accessed on: 30 May 2019.

135. PrescribeIT. *Canada's Electronic Prescription Service*. Available from: https://prescribeit.ca/component/edocman/165-prescribeit-patient-faq/view-document?Itemid=106. Accessed on: 24 October 2019.

136. Ocean eReferral Network. *About eReferrals 2019*. Available from: https://www.oceanereferralnetwork.ca/about/ Accessed on: 24 October 2019.

137. Canada Health Infoway. *Citizens' Perspectives*. Available from: https://www.infoway-inforoute.ca/en/what-we-do/research-and-insights/citizens-perspectives. Accessed on: 17 October 2019.

138. Population Australia. *Australia Population 2019*. 2019. Available from: http://www.population.net.au/. Accessed on: 10 April 2019

139. Government of Western Australia. *Overview of the Australian health system.* Available from: https://ww2.health.wa.gov.au/Careers/International-applicants/International-medical-graduates/Overview-of-the-Australian-health-system. Accessed on: 12 April 2019.

140. Health Direct. *Australia's healthcare system*. Available from: https://www.healthdirect.gov.au/australias-healthcare-system. Accessed on: 10 April 2019.

141. Department of Health Australian Government. *Privacy Policy*. 2017. Available from: https://www.health.gov.au/sites/default/files/doh-full-privacy-policy.pdf. Accessed on: 11 September 2019.

142. Australian Institute Of Health and Welfare. *Data on request*. 2018. Available from: https://www.aihw.gov.au/our-services/data-on-request. Accessed on: 10 April 2019

143. Australian Government. *About Us*. Available from: https://www.oaic.gov.au/about-us/. Accessed on: 10 April 2019.

144. Australian Digital Health Agency. *About the Agency*. Available from: https://www.digitalhealth.gov.au/about-the-agency. Accessed on: 11 September 2019.

145. Australian Government. *Health information and medical research.* Available from: https://www.oaic.gov.au/privacy-law/privacy-act/health-and-medical-research. Accessed on: 9 April 2019

146. My Health Record. *Legislation and Governance.* Available from: https://www.myhealthrecord.gov.au/about/legislation-and-governance. Accessed on: 10 April 2019.

147. Australian Government. *Federal Register Of Legislation.* 2012. Available from: https://www.legislation.gov.au/Details/F2016C00766. Accessed on: 9 April 2019.

148. Australian Govenrment National and Medical Research Council. *Australian Code for the Responsible Conduct of Research*. Available from: https://www.nhmrc.gov.au/sites/default/files/documents/attachments/grant%20documents/The-australian-code-for-the-responsible-conduct-of-research-2018.pdf. Accessed on: 12 April 2019

149. Office of the Australian Information Commissioner. *My HEalth REcords*. 2018. Available from: https://www.oaic.gov.au/privacy-law/other-legislation/my-health-records. Accessed on: 18 July 2019.

150. Australian Digital Health Agency. *Control access to your record*. Available from: https://www.myhealthrecord.gov.au/for-you-your-family/howtos/control-access-your-record. Accessed on: 11 December 2019.

151. My Health Record. *Remove Information*. Available from: https://www.myhealthrecord.gov.au/for-you-your-family/howtos/remove-information. Accessed on: 12 April 2019.

152. Healthcare in Europe. *E-health in Denmark*. 2018. Available from: https://healthcare-in-europe.com/en/news/e-health-in-denmark.html. Accessed on: 10 December 2019.

153. GDHP. *Improving Health Insights.* Available from: https://s3-ap-southeast-2.amazonaws.com/ehq-production-australia/5367c6f4cd970f2a170fd59895e7cc5ad18eeb56/documents/attachments/000/102/301/original/GDHP_PolicyEnv_2.04.pdf. Accessed on: 16 April 2019.

154. Australian Institute of Health and Welfare - METeOR. *Person-individual*

healthcare identifier, N(16). 2014. Available from: https://meteor.aihw.gov.au/content/index.phtml/itemId/432495. Accessed on: 19 August 2019.

155. Australian Digital Health Agency. *My Health Record system security*. Available from: https://www.myhealthrecord.gov.au/for-healthcare-professionals/howtos/my-health-record-system-security. Accessed on: 11 December 2019.

156. Michelle Sweidan. James Reeve. *Setting a standard for electronic prescribing systems.* Available from: https://www.nps.org.au/assets/71886b7cb2caa7ee-e28924dcb2b8-c069e5c4338703487bd94c4faf5ef4b9eb9b924f60ee4130e97710e7b321.pdf. Accessed on: 6 June 2019.

157. Australian Digital Health Agency. *eReferrals*. Available from: https://www.myhealthrecord.gov.au/for-healthcare-professionals/howtos/ereferrals. Accessed on: 11 September 2019.

158. European Commission. *Market study on telemedicine* 2018. Available from: https://ec.europa.eu/health/sites/health/files/ehealth/docs/2018_provision_marketstudy_telemedicine_en.pdf. Accessed on: 11 March 2019.

159. Worldometers. *Estonia Population* 2019. Available from: http://www.worldometers.info/world-population/estonia-population/. Accessed on: 1 May 2019.

160. World Health Organsialtion (WHO). *Estonia Health system review Vol. 20 No. 1 2018 Health Systems in Transition* Available from: http://www.euro.who.int/__data/assets/pdf_file/0011/377417/hit-estonia-eng.pdf?ua=1 Accessed on: 24 October 2019.

161. Ms Mari Matjus Mr Kaupo Lepasepp, Ms Mari Haamer,. *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/health/files/ehealth/docs/laws_estonia_en.pdf. Accessed on: 2 May 2019.

162. Wikidot. *E-health security and privacy*. Available from: http://e-health.wikidot.com/ehealth-in-estonia. Accessed on: 15 May 2019.

163. Health and Welfare Information Systems Centre. *An Overview of Current Estonian Health Information System Architecture Pitfalls and prospects* 2017. Available from: https://sam.lrv.lt/uploads/sam/documents/files/Veiklos_sritys/E.%20sveikata/priedas%20Nr_1_20171013_Estonian%20Health%20Information%20System%20overview.pdf. Accessed on: 24 October 2019.

164. Government of Estonia. *Interoperability services*. 2019. Available from: https://e-estonia.com/solutions/interoperability-services/x-road/. Accessed on: 24

October 2019.

165. E-Gov 2.0. *An Overview of Estonian E-Government Development and Projects*. 2015. Available from: http://egov2.eu/knowledge-base/an-overview-of-estonian-e%E2%80%91government-development-and-projects/. Accessed on: 19 August 2019.

166. Tervise ja Heaolu Infosüsteemide Keskus - Centre for Health and Welfare Information Systems. *Andmete kaitse - Data Protection*. Available from: https://www.tehik.ee/tervis/patsiendile/andmete-turvalisus/. Accessed on: 02 May 2019.

167. eHealth-Era. *eHealth Strategies-Estonia*. Available from: http://ehealth-strategies.eu/database/documents/Estonia_CountryBrief_eHStrategies.pdf. Accessed on: 11 May 2019.

168. . Artur Novek. *An Overview of Current Estonian Health Information System Architecture Pitfalls and prospects*. 2017. Available from: https://sam.lrv.lt/uploads/sam/documents/files/Veiklos_sritys/E.%20sveikata/priedas%20Nr_1_20171013_Estonian%20Health%20Information%20System%20overview.pdf. Accessed on: 14 May 2019.

169. e-estonia. *e-prescription*. 2019. Available from: https://e-estonia.com/solutions/healthcare/e-prescription/. Accessed on: 24 October 2019.

170. Medicum. *E-consultation and a digital referral* 2017. Available from: https://www.medicum.ee/en/uncategorized-en/e-konsultatsioon-ja-digisaatekiri/. Accessed on: 24 October 2019.

171. e-estonia. *e-Health Records*. Available from: https://e-estonia.com/solutions/healthcare/e-health-record/. Accessed on: 24 October 2019.

172. Eesti Haigekassa. *An increasing number of family physicians use e-consultation*. 2019. Available from: https://www.haigekassa.ee/en/uudised/increasing-number-family-physicians-use-e-consultation. Accessed on: 20 January 2020.

173. e-Governance Academy. *The Right Mix: How Estonia Ensures Privacy and Access to E-Services In The Digital Age*. 2018. Available from: https://ega.ee/news/the-right-mix-how-estonia-ensures-privacy-and-access-to-e-services-in-the-digital-age/. Accessed on: 24 October 2019.

174. Personal Communication Madis Tiik Former advisor of the President of Estonia in digital health area 06 June 2019.

175. Worldometers. *Finland Population (LIVE)*. 2019. Available from: http://www.worldometers.info/world-population/finland-population/. Accessed on: 15 May 2019.

176. Artur Olesch. *Finland: Digitalization Of Health Care Leads To Patient*

Empowerment. 2018. Available from: https://www.ictandhealth.com/news/finland-digitalization-of-health-care-leads-to-patient-empowerment/. Accessed on: 30 April 2019.

177. National Institute for Health and Welfare. *What is THL*. Available from: https://thl.fi/en/web/thlfi-en/about-us/what-is-thl-. Accessed on: 29 July 2019.

178. Kela. *With you throughout life – Supporting you through times of change* Available from: https://www.kela.fi/web/en/operations-kela-in-brief1. Accessed on: 24 October 2019.

179. Office of the Data Protection Ombudsman. *The Office of the Data Protection Ombudsman safeguards your data protection rights*. 2020. Available from: https://tietosuoja.fi/en/office-of-the-data-protection-ombudsman. Accessed on: 24 January 2020.

180. The Ministry of Social Affairs and Health. *Secondary use of health and social data* 2019. Available from: https://stm.fi/en/article/-/asset_publisher/sosiaali-ja-terveystietojen-tietoturvallinen-hyodyntaminen. Accessed on: 24 October 2019.

181. Finish institute for health and welfare. *Data permit Authority Findata*. 2019. Available from: https://thl.fi/en/web/thlfi-en/statistics/data-and-services/data-permit-authority-findata Accessed on: 24 October 2019.

182. DLA Piper. *Collection & Processing - Finland*. 2019. Available from: https://www.dlapiperdataprotection.com/index.html?t=collection-and-processing&c=FI. Accessed on: 16 May 2019.

183. Kanta. *Legislation*. Available from: https://www.kanta.fi/en/legislation. Accessed on: 1 May 2019.

184. Ministry of Health and Social Affairs. *Secondary use of health and social data*. 2019. Available from: https://stm.fi/en/secondary-use-of-health-and-social-data. Accessed on: 15 May 2019.

185. Government of Finland. *Frequently asked questions about the Act on Secondary Use of Health and Social Data* Available from: https://stm.fi/en/frequently-asked-questions-about-the-act-on-secondary-use-of-health-and-social-data. Accessed on: 24 October 2019.

186. Milieu LTD and Time.Lex. *Overview of the national laws on electronic health records in the EU Member States. National Report for Finland*. 2014. Available from: https://ec.europa.eu/health/sites/health/files/ehealth/docs/laws_finland_en.pdf. Accessed on: 29 August 2019.

187. Finnish Journal of eHealth and eWelfare. *Large-scale implementation and adoption of the Finnish national Kanta services in 2010–2017: a prospective, longitudinal, indicator-based study*. 2018. Available from: https://www.researchgate.net/publication/329435092_Large-scale_implementation_and_adoption_of_the_Finnish_national_Kanta_services_in_20

10-2017_a_prospective_longitudinal_indicator-based_study/fulltext/5c087f754585157ac1ab079e/Large-scale-implementation-and-adoption-of-the-Finnish-national-Kanta-services-in-2010-2017-a-prospective-longitudinal-indicator-based-study.pdf. Accessed on: 24 October 2019.

188. Kanta. *Patient Data Repository*. Available from: https://www.kanta.fi/en/professionals/patient-data-repository. Accessed on: 30 April 2019.

189. Teemupekka Virtanen. *The Healthcare and Number System in Finland*. 2014. Available from: https://www.fujitsu.com/downloads/JP/archive/imgjp/group/fri/events/conference/20140120virtanen.pdf Accessed on: 15 May 2019.

190. Kanta. *My Kanta Pages-Finland*. Available from: https://www.kanta.fi/en/my-kanta-pages. Accessed on: 1 May 2019.

191. Choosehealthcare.fi. *Finnish prescriptions*. 2019. Available from: https://www.choosehealthcare.fi/medicines/finnish-prescriptions/. Accessed on: 28 May 2019.

192. Kanta. *Acting on behalf of someone else*. Available from: https://www.kanta.fi/en/web/guest/acting-on-behalf-of-someone-else. Accessed on: 30 April 2019.

193. Sten Hankewitz. *Finnish e-prescriptions become valid in Estonia*. 2019. Available from: https://estonianworld.com/technology/finnish-e-prescriptions-become-valid-in-estonia/. Accessed on: 25 May 2019.

194. Ministry Of Health. *Healthcare in Denmark - An Overview*. 2017. Available from: https://www.healthcaredenmark.dk/media/1479380/Healthcare-english-V16-decashx-3.pdf. Accessed on: 2 December 2019.

195. Ministry of Health and the Elderly. *Data protection under the Ministry of Health and the Elderly*. 2019. Available from: http://sum.dk/Om-ministeriet/Databeskyttelse/Sundheds-og-aeldreministeriets-databeskyttelsespolitik.aspx. Accessed on: 28 November 2019.

196. Trifork. *One Patient - One National Medication Record*. 2019. Available from: https://trifork.com/?portfolio=fmk. Accessed on: 28 November 2019.

197. Datatilsynet. *About t he Danish Data Protection Agency*. 2019. Available from: https://www.datatilsynet.dk/english/about-us/. Accessed on: 10 December 2019.

198. Health Manangement. *The Danish Healthcare Quality Programme*. 2010. Available from: https://healthmanagement.org/c/hospital/issuearticle/the-danish-healthcare-quality-programme-ddkm. Accessed on: 10 December 2019.

199. MedCom. *About MedCom*. 2019. Available from: https://www.medcom.dk/medcom-in-english/about-medcom. Accessed on: 10

December 2019.

200. Sundhed. *Background*. 2019. Available from: https://www.sundhed.dk/borger/service/om-sundheddk/ehealth-in-denmark/background/. Accessed on: 10 December 2019.

201. The Danish Data Protection Agency. *The Act on Processing of Persona Data*. 2000. Available from: https://rm.coe.int/16806af0e6. Accessed on: 10 December 2019.

202. Milieu Ltd and Time.lex. *Overview of the national laws on electronic health records in the EU Member States. National Report for Denmark*. 2014. Available from: https://ec.europa.eu/health/sites/health/files/ehealth/docs/laws_denmark_en.pdf. Accessed on: 3 December 2019.

203. The Ministry of Health and the Elderly. *Background and vision for FMK*. 2019. Available from: https://sundhedsdatastyrelsen.dk/da/registre-og-services/om-faelles-medicinkort/baggrund-og-vision-fmk. Accessed on: 10 December 2019.

204. NordForsk. *Ethical review, data protection and biomedical research in the Nordic countries: A legal perspective* 2017. Available from: https://www.nordforsk.org/en/publications/publications_container/ethical-review-data-protection-and-biomedical-research-in-the-nordic-countries-2013-a-legal-perspective. Accessed on: 3 December 2019.

205. Ministry of Health and the Elderly. *Your Health Data; Patient Treatment*. 2019. Available from: https://sundhedsdatastyrelsen.dk/da/borger-og-offentlighed/dine-sundhedsdata/patientbehandling. Accessed on: 3 December 2019.

206. Ministry of Health and the Elderly. *Data protection under the Ministry of Health and the Elderly*. 2019. Available from: http://sum.dk/Om-ministeriet/Databeskyttelse.aspx. Accessed on: 3 December 2019.

207. National Centre for Register-based Research. *Danish Registers*. 2019. Available from: https://econ.au.dk/the-national-centre-for-register-based-research/danish-registers/. Accessed on: 10 December 2019.

208. Ministry of Health and the Elderly. *Department's processing of personal data*. 2019. Available from: http://sum.dk/Om-ministeriet/Databeskyttelse/Personoplysninger/Personoplysninger-til-Statistik-analyse.aspx. Accessed on: 10 December 2019.

209. Copenhagen Healthtech Cluster. *National Patient Register*. 2019. Available from: https://www.danishhealthdata.com/find-health-data/Landspatientregisteret. Accessed on: 10 December 2019.

210. OECD. *OECD Reviews of Health Care Quality: Denmark*. 2013. Available from: https://www.oecd.org/els/health-systems/ReviewofHealthCareQualityDENMARK_ExecutiveSummary.pdf. Accessed on:

02 December 2019.

Health Information and Standards Directorate
Health Information and Quality Authority
Unit 1301, City Gate,
Mahon,
Cork
T12 Y2XT