HISO 10064:2017

Health Information   
Governance Guidelines

August 2017

**Document information**

HISO 10064:2017 Health Information Governance Guidelines

ISBN 978-1-98-850275-5 (online)

Published in August 2017 by the Ministry of Health

Health Information Standards Organisation (HISO) standards are published by the Ministry of Health for the New Zealand health and disability sector.

This document is available at http://www.health.govt.nz/our-work/ehealth/digital-health-standards-and-governance/health-information-standards/approved-standards

**Contributors**

|  |  |
| --- | --- |
| Dr Sandra Hicks  New Zealand Medical Association | Denise Irvine  New Zealand Nurses Organisation and College of Nurses |
| Sebastian Morgan-Lynch  Office of the Privacy Commissioner | Stephanie Fletcher  Chair, NHITB Consumer Panel |
| Dr Inga Hunter  General Practice New Zealand and Royal New Zealand College of General Practitioners | Sharron Cole (resigned March 2014  Midwifery Council of New Zealand |
| Dr Lyndy Matthews  Council of Medical Colleges | Barbara Phillips – Delegated to Phil Knipe (from March 2013)  Ministry of Health |
| Julia Fomison from May 2014  Canterbury DHB | Fiona Thomson from July 2014.  General Practice New Zealand |

**Copyright**

|  |  |
| --- | --- |
| **CCBY** | This work is licensed under the Creative Commons Attribution 4.0 International licence. In essence, you are free to: share ie, copy and redistribute the material in any medium or format; adapt ie, remix, transform, and build upon the material. You must give appropriate credit, provide a link to the licence and indicate if changes were made. To view a copy of this licence, visit <http://creativecommons.org/licenses/by-nd/4.0/> |

**Keeping standards up to date**

HISO standards are regularly updated to reflect advances in health information science and technology. See the Ministry of Health website at health.govt.nz for information about the standards development process. We welcome your ideas for improving this standard. Email standards@health.govt.nz or write to HISO, Ministry of Health, PO Box 5013, Wellington 6140.

Contents

1 Purpose 5

1.1 Why these Guidelines are important 5

1.2 How to use these Guidelines 6

1.3 History 6

1.4 What is information governance? 6

1.5 Ownership of information 7

1.6 Definitions 7

1.7 Requirements 8

2 Maintaining quality and trust 9

2.1 Objective 10

2.2 Policy statements 10

2.3 Data quality 11

2.4 Managing information privacy policy 12

2.5 Code of conduct 13

2.6 Privacy complaints and breach of privacy procedure 14

2.7 Privacy impact assessments 14

3 Upholding consumer rights and maintaining transparency 16

3.1 Objective 16

3.2 Policy statements 16

3.3 Health literacy 17

3.4 Information on privacy, patient notification and consent 18

3.5 Rights of access and correction 19

3.6 Training and education 21

3.7 Audit logs and proximity reports 21

3.8 Patient portals 22

4 Appropriate disclosure and sharing 24

4.1 Objective 24

4.2 Policy statements 24

4.3 Consumer preferences for sharing information through shared care and electronic health record systems 25

4.4 Disclosure outside the health and disability sector 27

4.5 Secondary use of information 28

4.6 Access control 29

4.7 Role-based access control 30

4.8 Resource 31

5 Securing and protecting personal health information 32

5.1 Objective 32

5.2 Policy statements 32

5.3 Use of cloud or hosted services for managing health information 33

6 Governance and implementation of these Guidelines 35

Appendix 1: Compliance checklist 36

Appendix 2: Relevant legislation 39

Appendix 3: Definitions 42

Appendix 4: Key information governance principles 48

Appendix 5: Privacy access escalation ladder 51

Appendix 6: Privacy fact sheet 53

Appendix 7: Privacy poster 56

Appendix 8: Code of conduct to safeguard the privacy and confidentiality of patient health information 57

Appendix 9: Privacy impact assessments 59

Appendix 10: Disclosure to third parties 63

Appendix 11: Information matching 67

Appendix 12: Approved information sharing agreement 68

Appendix 13: Secondary use of data 70

Appendix 14: Example of role based access control matrix 73

# Purpose

The Health Information Governance Guidelines provides 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.

Dovetailing into these Guidelines is the [Health Information Security](http://healthitboard.health.govt.nz/system/files/documents/publications/hisf_update_dec_2015.pdf) Framework, which provides policy guidance on securing health information. The two are strongly intertwined. How information can be held secure, however, is a large field of its own, and rather than repeat here what is said under HISO 10029:2015 Health Information Security Framework[[1]](#footnote-1), it is recommended that the Security Framework and this guidance be read together.

## Why these Guidelines are important

Our health system continues to demand higher levels of information use to achieve better health care. In response to this demand, health practitioners have increased their use of technology and are sharing the information they need with each other electronically. While this makes sharing health information easier and more reliable, greater attention must be given to ensuring consumer and health provider trust in systems is maintained.

The Health Information Governance Guidelines (the Guidelines) provides essential policies and guidelines on how to share health information safely. It sets out how health providers, working in partnership with consumers, can share information legitimately in the performance of their duties without infringing patients’ rights to privacy. Safe sharing involves building on good cultural practices around trust in information, alongside changes to processes and practices, and technical enhancements to health information systems.

Health providers are not expected to be information governance experts. The Privacy Act 1993 and Health Information Privacy Code 1994 have set out the principles of how health information should be collected, stored, corrected, disclosed and disposed of, but do not provide a detailed set of guidelines on how to apply the principles in practice. As a consequence each DHB, community health provider and IT vendor applies their own approach to health information governance, which can lead to duplication, uncertainty and misinterpretation of health information-related policies and legislation.

It is important to strike the right balance between easy access to information and constraints on information sharing. Taking an approach which is too conservative in the sharing of information can lead to undesirable outcomes for patients and ongoing inefficiencies in the health system. Conversely, making information too easily accessible risks privacy breaches and a loss of consumer and provider trust.

These Guidelines respond to key questions which have persisted in the sector for many years. What types of access controls do I need to have in my systems? Can a patient opt-off collecting or sharing information? When is it appropriate to disclose information without the direct consent of the patient? What are the consumer’s rights and expectations over their health information?

These Guidelines apply to any health provider that collects, stores, uses or comes into contact with personal health information.

## How to use these Guidelines

These Guidelines sets out the policies and procedures for health providers who collect and share personal health information. It uses a structured language and set of concepts within which to think about the governance of health information.

The policies are set out under four major subject areas:

* Maintaining quality and trust
* Upholding consumer rights and maintaining transparency
* Appropriate disclosure and sharing
* Securing and protecting personal health information.

Each subject area provides the legal and policy context, and then a set of tangible requirements which are auditable. A compliance checklist is included in Appendix 1.

How these Guidelines will be governed and adopted by the sector is discussed in Chapter Nine.

Supporting resources and important references are included in the appendices.

## History

The need for some Guidelines[[2]](#footnote-2) arose from the requirements of the first National Health IT Plan in 2010 (IT Plan 2010) following consultation with the sector. As a result the Health Information Governance Expert Advisory Group (HIGEAG) was created. HIGEAG had its first meeting in June 2012.

HIGEAG also developed a paper on the withholding of health information. This looked into how consumers could control access to their health information in a shared information ecosystem. The key findings from this paper have been incorporated into these Guidelines.

## What is information governance?

Information governance[[3]](#footnote-3) provides a means of bringing together all the relevant legislation, guidance and evidence-based practice that apply to the handling of information and offers a consistent way for people working in health and social care to deal with the many different legal provisions, guidance, and professional codes of conduct that apply to handling personal health information.

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

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

Governing the collection, use and disclosure of personal health information needs to be led from the top. The culture needs to be focused on ways of appropriately sharing health information. In this way, information governance can and should become a source of knowledge and guidance for staff. Information governance needs to be more than the responsibility of just one person within an organisation. It should also not be seen solely as a defensive role the organisation takes on.

## Ownership of information

Historically, there has been debate over who owns the information contained within the patient information system. A patient might consider they own any information relating to their health while a health practitioner may consider that any notes they record about the patient as a result of a medical examination belong to them, or may state that ‘the patient owns their own information’ as a way of expressing how carefully it will be managed.

The Privacy Commissioner has said that rather than thinking in terms of “property” ownership, it is more accurate to say:

“People have rights over health information about themselves and health agencies have obligations over the health information they hold. Rule 6 [of the Health Information Privacy Code 1994] gives individuals the right to access information about themselves and rule 7 gives them the right to seek correction of that information if they think it is inaccurate or misleading.”[[4]](#footnote-4)

## Definitions

A full list of definitions of key terms can be found in Appendix 3.

Many terms will be familiar to those who work in the health and disability sector, however there are some important distinctions to be made amongst commonly used terms.

‘Health provider’ describes an organisation or a person involved in the provision of health care services. An individual health provider can be either a registered health practitioner (which is a term defined in the Health Practitioners Competence Assurance Act 2003) or a health worker (a person who works in health services who is not registered under that Act).

‘Health information’ or ‘personal health information’ refers to information associated with an individual. Anonymous or aggregated data (ie, data that does not directly identify an individual) is not regulated in law.[[5]](#footnote-5) A subset of health information is the health record, which is the record of an individual’s health care, and which may be kept in multiple files, and in either electronic or paper form.

Sometimes non-personal health information may be mixed with health information. Where this happens the non-personal health information should be treated as health information for the purposes of these protocols.

‘Point-of-care information systems’ are those that hold the master copy of the patient’s information for that point-of-care health provider. An example is a practice management system. A shared care information system is designed to share health information across providers by accumulating data from point-of-care systems and allowing health providers to access that data or health information through a secure online portal.

## Requirements

The requirements set out under each subject area in these Guidelines contain the core information governance requirements expected of all health providers and are based on the key principles underpinning these Guidelines. A copy of the principles can be found in Appendix 4.

The subject areas are:

* Maintaining quality and trust – this chapter sets out how these Guidelines will support information sharing to enable health practitioners to have access to relevant and high-quality information at point of care, while assuring consumers their personal health information remains confidential.
* Upholding consumer rights and maintaining transparency – this chapter sets out consumers’ privacy rights in regard to their personal health information and the requirement that all health agencies maintain transparency in their use of personal health information.
* Appropriate disclosure and sharing – this chapter sets out the rules for information sharing and disclosure.
* Securing and protecting personal health information – this chapter sets out the minimum requirements for securing and protecting personal health information in storage or in transit.
* Governance and implementation of these Guidelines.

# Maintaining quality and trust

Maintaining quality and trust in health information is critical for both health practitioners and consumers. Trusted health information allows the health practitioner to accurately understand the consumer’s health status, make well-informed decisions and co-ordinate care with other health providers. The same information provides the consumer with the story of their health care and their journey through the health system.

Good health records are essential for the continuity of care of the patient. They enable the health practitioner to reconstruct the essential parts of each patient contact without reference to memory. They should therefore be comprehensive enough to allow a fellow registered health practitioner to either carry on where the previous practitioner left off, or use the information contained in the record as a basis for any subsequent course of treatment or care.[[6]](#footnote-6),[[7]](#footnote-7)

Increasingly, care for consumers is delivered by a virtual team operating in many care settings. Electronic health records create the platform for the sharing of health information across a wide set of supporting health providers.

A workable balance between health practitioner rights and consumer rights to access information needs to be put into practice to ensure consumers maintain some level of control over their information.

Consumers want good quality care. They also want their privacy protected. Most consumers are comfortable that health providers share their information with other providers for the purposes of treatment and care.[[8]](#footnote-8)

The trust consumers have in the health care system is enhanced when their health information is managed well. A badly managed privacy breach affects the confidence of both consumers and health practitioners.[[9]](#footnote-9) Without sufficient transparency and controls over access to health information, trust in the system is eroded.[[10]](#footnote-10)

To maintain trust and confidence, health providers need to be transparent about how personal health information is used. In particular, if asked, a health provider should be able to make available to the consumer evidence of who has seen their information, when, where and for what purpose. Giving consumers some ability to control access rights will also foster greater trust in the health system.

## Objective

Consumers trust their health provider to treat their health information confidentially and are comfortable with all relevant health information being available to other health providers for the purposes of treatment and care.

## Policy statements

Information held is kept accurate, up-to-date and as relevant as is necessary for the purposes of treatment and care.

All health information is treated as MEDICAL IN CONFIDENCE.[[11]](#footnote-11)

Personal health information shall only be discussed in appropriate settings.

Use of health information is clear and evident to the consumer. It is accessed only by persons who have authorised access in the performance of their duties.

Health information remains under the jurisdiction of the health and disability sector unless authorised by law or the consumer has explicitly given their permission for its release.

|  |  |
| --- | --- |
| **Relevant Health Information Privacy Code Rules[[12]](#footnote-12)** | |
| Rule 1 | Health information must only be collected when:   * the collection is for a lawful purpose, connected with what the agency does, and * it is necessary to collect the information for that purpose. |
| Rule 4 | Health information must not be collected by unlawful means or by means that are unfair or unreasonably intrusive in the circumstances. |
| Rule 8 | Before it uses or discloses health information, an agency must take reasonable steps to check that information is accurate, complete, relevant, up-to-date and not misleading. |
| Rule 10 | Agencies must use health information for the same purpose for which they obtained that information.  Other uses are occasionally permitted (for example, because this is necessary to prevent or lessen a serious threat, enforce the law, or if the use is directly related to the purpose for which the agency got the information). |

## Data quality

### Policy

Health records maintained electronically enable high-quality structured information to be collected and retained for later re-use. The quality of information available at the point of care contributes to the quality of care delivered to the consumer. Electronic health record systems support better clinical decision-making, process flow and co-ordination of care. Furthermore, the captured information contributes towards the long-term improvement of the health system through data analytics.

The quality of information is a product of its accuracy, validity, reliability, timeliness, relevance, legibility and completeness. The benefits of good quality data include:

* consumers are more likely to receive safe and effective care if health providers have access to accurate and reliable information to support decision-making
* consumers are more likely to receive safer and better care if activity data used to support quality improvement is of good quality and reflects actual delivery
* consumers will have access to reliable information to help them decide where to access care
* if the information used to support decision making is of a high quality, health care services can plan and provide for population needs more effectively and efficiently, eg, good quality demographic data that highlights an aging population or a significant increase in immigrants in a specific catchment area can facilitate services in planning for the specific needs of that area
* health care research contributes to improved outcomes by providing evidence to support particular care processes. This research can only be relied on if it is based on good quality information.[[13]](#footnote-13)

### Requirements

It is expected all health records comply with:

* New Zealand Standards requirements in relation to health records[[14]](#footnote-14) (policy)
* the Health (Retention of Health Information) Regulations 1996 which requires Identifiable health information to be kept for a minimum of 10 years[[15]](#footnote-15) (law)
* rule 9 of the Health Information Privacy Code 1994 which requires that health information must not be kept for longer than required[[16]](#footnote-16) (law)
* the governing General Disposal Authority, where information is held by a public sector agency that is subject to the Public Records Act 2005 (policy/law)
* health providers have a procedure for managing the co-existence of paper and electronic records (policy).

The procedure for managing the co-existence of paper and electronic records must cover:

* which record is the master record
* the management of the paper record once the electronic record becomes the master record
* how updates to the master record are managed.

Health information systems should build in master data management for identity and core reference datasets. Real time interfaces should be developed for:

* NHI number and patient demographics via the National Health Index (policy)
* NZ Universal List of Medicines (NZULM) for whenever medications are referenced
* Health Provider Index for health organisations, locations and health practitioners (real time interface still in development).

Health information systems should adopt Health Information Standards Organisation (HISO) standards for the exchange of health information (policy).

Health information systems should use HISO standards[[17]](#footnote-17) for storing content or core reference datasets:

* New Zealand Pathology Observation Codes (NZPOCS)
* Ethnicity Level 4.

### Resources

For further information on the management of health records see:

* Coles Medical Practice in New Zealand 2013 edition,[[18]](#footnote-18) in particular chapter 13 “Medical Records and Patient Access to Information”
* “The Maintenance and Retention of Patient Records”, MCNZ Fact Sheet August 2008[[19]](#footnote-19)
* The Public Records Act 2005 (relevant for DHBs)
* New Zealand Standard 8153:2002.[[20]](#footnote-20)

## Managing information privacy policy

Part of ensuring health providers maintain the trust of consumers is to have robust and well-governed procedures for managing privacy. Technical tools such as Role Based Access Control and Proximity Audits are considered in more detail later in this document.

Information systems should incorporate privacy settings into their functionality:

* by recording the relationship of the health provider to the patient, for example, through enrolment into a health service
* by recording direct consent or reason for access
* by recording information which associates the health provider to the patient through proximity, for example, admission to a surgical ward creating an implied consent for those working there.

### Requirements

Health providers have a designated privacy officer who has responsibility for information governance and privacy issues.[[21]](#footnote-21)

Health providers have in place clear policies and procedures covering the collection, use, disclosure, storage and access to personal health information (policy).

Job descriptions, employment contracts and formal contractual arrangements include the need for compliance with information governance policies and procedures by all persons, groups and health practitioners carrying out work on behalf of the health provider (policy).

Health providers ensure there is a process in place to actively monitor information governance policies and procedures, and review adverse incidents thus ensuring that effective remedial and preventative action is taken[[22]](#footnote-22) (policy). Any breaches and or ‘near misses’ are managed in accordance with the breach and complaints policy (law).

Health providers ensure that all new information systems and processes are risk assessed to ensure that they comply with the Privacy Act and Health Information Privacy Code. For example, they should undertake a privacy impact assessment (policy).

### Resources

The Office of the Privacy Commissioner has produced a Privacy Escalation Ladder which provides guidance on when identifiable information can be disclosed. A copy of this can be found in Appendix 5.

A Privacy Fact Sheet can be found in Appendix 6. This covers the key purposes for which information is collected in a health context.

A privacy poster which can be displayed in public waiting rooms can be found in Appendix 7.

Guidance on writing privacy impact assessments can be found in Appendix 9.

## Code of conduct

A code of conduct is a set of [rules](http://en.wikipedia.org/wiki/Procedural_law) outlining the responsibilities of, or proper practices for employees and contractors working for, a health provider. It sets out the expectations of the health provider for its staff.

### Requirements

All health providers have a code of conduct which sets out employees’ and contractors:

* duty of confidentiality
* obligations in respect of the Privacy Act 1993 and Health Information Privacy Code 1994 (policy).

### Resources

A sample code of conduct covering the obligations of privacy and confidentiality in respect of patient health information has been prepared by Canterbury DHB and can be found in Appendix 8.

## Privacy complaints and breach of privacy procedure

The way health organisations manage complaints and potential or actual breaches of privacy is important. When there is a breach or complaint, the health organisation must have a formal and transparent way of handling it. This is important for maintaining trust and confidence.

### Requirements

All health providers have a policy to manage privacy complaints and breaches of privacy. The policy must cover the four issues of:

* breach containment and preliminary assessment
* evaluation of the risks associated with the breach
* notification
* prevention (policy).

Any deliberate access of another person’s health record without consent or good cause will generally be treated as serious misconduct (policy).

### Resources

For guidance on how to deal with privacy breaches refer to the Office of the Privacy Commissioner’s “Data Safety Toolkit”.[[23]](#footnote-23)

## Privacy impact assessments

A Privacy Impact Assessment (PIA) is a systematic process for evaluating a proposal in terms of its impact upon privacy. A PIA helps to:

* identify the potential effects that a proposal may have upon individual privacy
* examine how any detrimental effects upon privacy might be overcome
* ensure that new projects comply with the information privacy principles.[[24]](#footnote-24)

The benefits of a privacy impact assessment have been described by the Office of the Privacy Commissioner as follows:

“Privacy Impact Assessment can operate as an ‘early warning system’ for businesses and government organisations. It can help management make better informed decisions and avoid a privacy disaster. No chief executive wants to see his or her organisation’s exciting new product or initiative panned in the news media as a danger to customer privacy. While favourable publicity can never be guaranteed, acting on a privacy impact report improves the chances that any privacy headlines are good news for the business rather than a public relations (and possibly share price) disaster.”[[25]](#footnote-25)

For further information on privacy impact assessments and links to relevant resources see Appendix 9.

### Requirements

Health providers undertake a Privacy Impact Assessment whenever they propose to introduce a significant new system (electronic, manual or a combination of both) that affects access to or exchange of personal health information. Any risks identified are addressed (policy).

# Upholding consumer rights and maintaining transparency

Consumers’ rights over their health information are protected through privacy legislation and codes of practice. These uphold the right of consumers to know what their information is used for, and to obtain access to, and request correction of, their information.

This section sets out consumers’ rights as well as ways in which health providers must make the sharing of information transparent. ‘Transparent’ in these Guidelines means that not only is the sharing of health information traceable but that consumers understand the information they are provided with. Health literacy is a key part of transparency. In particular, health providers should use plain language to improve consumer understanding.

## Objective

Consumers understand they have information privacy rights and what those rights are. These Guidelines will support and uphold these rights.

## Policy statements

Consumers shall not be refused urgent treatment solely on the basis that they do not have adequate evidence of identity or eligibility.[[26]](#footnote-26)

Health providers will tell consumers why they are collecting their personal health information and how it is likely to be used.

A consumer may access and have a copy of their health information. They are also entitled to know who has accessed it.[[27]](#footnote-27)

A consumer may ask for their health information to be corrected. The health provider must consider the request and either make the correction sought, or advise the consumer that the correction is not to be made but that the consumer has the right to have a copy of the proposed correction appended.

Health communications and services should be structured around the assumption that every patient has limited health literacy (a ‘universal precautions’ approach).

|  |  |
| --- | --- |
| **Relevant Health Information Privacy Code Rules** | |
| Rule 2 | Health information must usually be collected from the person who the information is about. But sometimes it is all right to collect information from other people instead – for instance, when:   * getting it from the person concerned would undermine the purpose of the collection * compliance would prejudice the interests of the individual concerned, or the safety of any individual * it is necessary so a public sector body can uphold or enforce the law * the person concerned authorises collection from someone else. |
| Rule 3 | When an agency collects health information from the person the information is about, it has to take reasonable steps to make sure that person knows things like:   * why it is being collected * who will get the information * whether the person *has* to give the information or whether this is voluntary * what will happen if the information isn’t provided. |
| Rule 6 | People have a right to ask for access to health information about themselves. Agencies can refuse to give access in some situations, for instance because giving the information would:   * endanger a person’s safety * prevent detection and investigation of criminal offences * involve an unwarranted breach of someone else’s privacy.[[28]](#footnote-28) |
| Rule 7 | People have a right to ask the agency to correct information about them, if they think it is wrong.  If the agency does not want to correct the information, it does not usually have to. However, people can ask the agency to add *their* views about what the correct information is. |

## Health literacy

### Policy

Health literacy is the ability to obtain, process, and understand health information to make informed decisions about health care.[[29]](#footnote-29)

Medical language often uses complex terminology and can be difficult to understand. Similarly the forms consumers are required to complete can often be confusing. Health providers should adopt a universal precautions approach to health literacy. Health communications and services should be easy to understand.

### Requirements

All health providers adopt a universal precautions approach in all communications with consumers and patients (policy).

### Resources

The Ministry of Health has produced a framework for health literacy which can be found at <https://www.health.govt.nz/publication/framework-health-literacy>

The US Agency for Healthcare Research and Quality has produced a ‘Health Literacy Universal Precautions Toolkit’ for health practitioners. It is particularly aimed at primary care but is useful to all health practitioners.[[30]](#footnote-30)

Plain language explanations should be included in patient portals.

## Information on privacy, patient notification and consent

Health providers need to tell consumers why they are collecting their health information and who the providers are likely to share it with. This means that health providers need to either know how a patient’s information is travelling through the health system or at least know where to find this out for the patient.

The consumer can be informed through having a privacy fact sheet prominently displayed and available for them to read. The health provider should also be familiar with the fact sheet so they can answer any questions the consumer may have on privacy.

In some circumstances a fact sheet may not be sufficient. For example, where a health practitioner obtains a second opinion from a specialist who the patient would not normally expect the health practitioner to contact in the usual course of consultation. In such situations the health provider should first discuss with their patient their intention to obtain the second opinion and obtain their authorisation to do so.

### Privacy requirements

Health providers should have available up-to-date and accurate information for consumers about their rights and the use of personal health information.[[31]](#footnote-31) This should be displayed prominently (policy/law).

Health providers should be familiar with the privacy fact sheet and able to answer consumer queries about the range of people or agencies their information is shared with (policy).

### Resources

A privacy fact sheet and poster which can be used by the Health and Disability Sector, can be found in Appendix 6 and Appendix 7.

### Patient notification and consent requirements

Health providers have documented a privacy policy that is available for consumers to see. The policy supports consumers’ rights under the Privacy Act 1993 and Health Information Privacy Code 1994. The policy is regularly reviewed (policy).

### Resources

The Office of the Privacy Commissioner has produced a Privacy Escalation Ladder which provides guidance on when identifiable information can be disclosed. A copy of this can be found in Appendix 5.

## Rights of access and correction

### Access requests by consumers

Under rule 6 of the Health Information Privacy Code, health providers who hold information about a consumer in a way that is readily retrievable must provide that consumer with access to the information if requested.

### By parents

Section 22F of the Health Act 1956 provides that health information must be disclosed, on request, to the individual’s representative or any person providing health or disability services to the individual.

The parent or guardian of a child under 16 years is their representative.

Where the person holding the information reasonably believes that a disclosure of health information about a child under 16 to his or her parent or guardian would be against the child’s wishes or interests, the request may be refused. Requests may also be refused on the withholding grounds in sections 27–29 of the Privacy Act.

Children under 16 do not have a veto over disclosure of information to their parents. Whether a health provider will accede to a child’s request that health information about them not be disclosed is within their discretion. In considering the request they should take into account the relative maturity of the child and the severity of the health matter under discussion.

### 16 years and older

Under the law a child is deemed competent from the age of 16 onwards (unless factors determine otherwise). At that point the parent no longer has the right to see their child’s health record without their authorisation.

### By a person who is intellectually disabled or their carer

A person with an intellectual disability has the right to see their shared record. A representative of that person, being someone lawfully acting on their behalf, may also seek access to their health record under section 22F. Access should be granted to a representative unless the disclosure would be against the wishes or interests of the person concerned, having regard to the competence of the person and the consequences if access is granted or refused.

### Right of correction

Consumers have the right to ask that any information held on them is corrected. If the information is not amended, the consumer has the right to have their statement of correction attached to their health record.[[32]](#footnote-32)

### Requirements

Health providers must help facilitate access and correction requests when they are made[[33]](#footnote-33) (law).

Parents or guardians and other health providers shall be allowed to see their child’s health record if the child is under 16, unless:

* the child does not want the information disclosed, and
* the health practitioner considers it appropriate to accede to the child’s request having regard to the relative maturity of the child and the severity of the health matter under discussion (law).

Parents or guardians shall be allowed to see their child’s health record unless it is not in the child’s best interests (law).

Any request for access or correction is dealt with promptly and a decision on that request is made not later than 20 working days after the request was made. If the health provider requires an extension of time to complete the request, they must give notice of the extension to the consumer who made the request within 20 working days after the day on which the request is received[[34]](#footnote-34) (law).

The notice:

* specifies the period of the extension
* gives the reasons for the extension; and
* states that the consumer who made the request for the information has the right to make a complaint to the Privacy Commissioner about the extension[[35]](#footnote-35) (law).

Where a consumer makes a request for correction of their personal health record and the health provider determines that the correction should not be made, they advise the consumer of:

* its decision, the reasons why the correction was not made, and any supporting grounds for that refusal[[36]](#footnote-36) (law)
* the consumer’s right to have a statement of the correction sought but not made appended to the health record[[37]](#footnote-37) (law)
* the consumer’s right to complain to the Privacy Commissioner and to seek an investigation and review of that decision[[38]](#footnote-38) (law).

## Training and education

It is expected that all health providers offer appropriate training in information management to their staff.

The importance of sharing health information when appropriate, and protecting the health information privacy of patients and consumers in all other circumstances, needs to be embedded in the culture of health providers.

Training and education should be consistent across all occupations or professions. In addition, the use of multi-disciplinary and multi-agency training could help improve health providers’ understanding of information management issues faced by their peers.

### Requirements

Health providers must provide appropriate training and education to staff on privacy and the appropriate sharing of data (policy).

### Resource

The Office of the Privacy Commissioner has prepared some e-learning privacy training modules. These can be found at <https://www.privacy.org.nz/further-resources/online-privacy-training-free/>

## Audit logs and proximity reports[[39]](#footnote-39)

As the use of electronic systems to manage health care information becomes the norm, it is important transparency of access is in place to ensure the confidence of consumers in the health system. One way to do this is by logging accesses to a consumer’s health record and making the audit log access and proximity report available to consumers.

### Requirements

All point-of-care and shared care clinical information systems must maintain an audit log of all enquiries, modifications, additions, or deletions to health records. The log must also maintain a record of all users who have logged into the system, and a record of all reports, data exchange interfaces and/or extracts performed through the software (policy).

The audit record of each access or change must show:

* the date and time of the access or change
* the location, user identifier and role of the person accessing or changing the data
* the function being performed (screen name, menu selection or process within the application)
* any additional information on the reason for access, such as, ‘break glass’,[[40]](#footnote-40) informed consent, etc (policy).

The audit log shall be kept for a minimum of two years (policy).

Health providers shall review the audit log at least monthly, and shall investigate all apparent outliers and break glass accesses.

Health providers must be able to provide consumers with either a paper or electronic copy of the audit log if requested (policy).

## Patient portals

Patient portals enable consumers to access their own health information and this empowers them to take more ownership of their health care.

The potential benefits of a patient portal include:

* patients can self-manage aspects of their health care such as booking appointments and ordering repeat medications online
* patients are better informed and can have more input into their treatment
* patients records will be accurate and up to date
* patients can engage with clinicians cord clinical information on the portal leading to better management of chronic conditions
* better use of consumers’ and health providers’ time
* patients will be more aware if requested tests or results are not carried out or followed up, and are able to raise this with clinicians.

### Requirements

A patient portal should:

* meet the HISO 10029 Health Information Security Framework standard: <http://healthitboard.health.govt.nz/system/files/documents/publications/hisf_update_dec_2015.pdf>
* be available to all of the health provider’s eligible registered patients (policy).

Any patient portal should also have the capability to allow patients to:

* have a single sign on to access all functions
* view their medical records from their general practice
* send and receive secure messages
* access a number of online services such as:
* requesting repeat prescriptions
* booking online appointments
* receiving recall reminders
* viewing lab results
* managing health goals, setting up tasks and tracking results
* viewing the audit log of all accesses
* allowing patients to create accesses by delegates to their notes should they choose (policy).

The health provider shall provide education and training to its staff on use of the patient portal system (policy).

The health provider shall have a policy on staff access to patient portals which is compliant with the Privacy Act 1993 and Health Information Privacy Code 1994 (policy).

Health providers should ensure the consumer is aware of any sensitive reports or results before this information is placed in their patient portal (policy).

# Appropriate disclosure and sharing

The health and disability system is increasingly delivering care to patients in different physical locations and settings. Where there is a ‘virtual team’ supporting the patient, the health record needs to be accessible and shared across different health providers and in different settings. In the New Zealand Health Strategy, “the theme of ‘one team’ is about operating as a team in a high-trust system that works together with the person and their family and whānau at the centre of care”.[[41]](#footnote-41) The system needs to both enable relevant health information to be available, and manage inappropriate disclosure or sharing to preserve the trust of consumers.

When determining whether or not to access or share personal health information, the Privacy Commissioner’s Access Escalation Ladder can be helpful. A copy of this can be found in Appendix 5. In summary the questions that should be asked, in ascending order are:

* Can the provider get by with anonymous information?
* Has the person agreed to this?
* Has the person been told? (May be sufficient where obtaining consent is not practical and using or disclosing the information this way is in line with the purpose for which it was obtained).
* Is there a serious threat or a ‘break glass’ situation?
* Is there another legal provision that can be relied on (eg, an approved Information Sharing Agreement – ‘AISA’)?

This section sets out the requirements in terms of appropriate disclosure and sharing, and covers issues of access control, requests for disclosure by third parties, Approved Information Sharing Agreements (AISAs), information matching and secondary use of information.

## Objective

Health providers and their employees, contractors or agents have a clear understanding of who may access personal health information, when and for what reason.

## Policy statements

A health provider may use or disclose a consumer’s health information in the course of their duties provided:

* the purposes for which the information is used have been communicated to the consumer
* they have the consumer’s direct consent, or
* they have the consumer’s implied consent because the consumer has enrolled in, registered with, or has been admitted to the service, or
* they have been authorised by law to do so.

A consumer’s choice not to disclose information shall not be used as an excuse for withholding treatment. A practitioner may however refuse to provide treatment if they feel it is unsafe to treat the patient in the circumstances.

Custodians and stewards of health information should have confidence in and where necessary seek assurance in writing from the other agency that they have the ability to protect the information from unauthorised access, use, modification or disclosure before forwarding it to that agency.[[42]](#footnote-42)

|  |  |
| --- | --- |
| **Relevant Health Information Privacy Code Rules** | |
| Rule 3 | When an agency collects health information from the person the information is about, it has to take reasonable steps to make sure that person knows:   * why it is being collected * who will get the information * whether the person *has* to give the information or whether this is voluntary * what will happen if the information isn’t provided. |
| Rule 5 | Agencies must ensure there are reasonable safeguards in place to prevent loss, misuse or disclosure of health information. |
| Rule 10 | Agencies must use health information for the same purpose for which they obtained that information.  Other uses are occasionally permitted (for example because this is necessary to enforce the law, or the use is directly related to the purpose for which the agency got the information). |
| Rule 11 | Agencies can only disclose health information in limited circumstances. One example is where another law requires them to disclose the information. Also, an agency can disclose information if it reasonably believes, for example, that:   * disclosure is one of the purposes for which the agency got the information * disclosure is necessary to uphold or enforce the law * disclosure is necessary for court proceedings * the person concerned authorised the disclosure * the information is going to be used in a form that does not identify the person concerned. |

## Consumer preferences for sharing information through shared care and electronic health record systems

Where personal health information is transferred to or made available through a shared care system, the consumer should have control over their information sharing preferences with the guidance of their health practitioner. This may take the form of withholding their entire health record from a shared care system and only disclosing their information to their chosen health provider. Alternatively, they may choose to include their information in a shared care system but withhold certain parts which they deem sensitive, for example, a diagnosis/problem associated with mental health or sexual health. The fact that all or some information has not been disclosed will be transparent to a health provider using the system.[[43]](#footnote-43)

As regional and national electronic health record systems continue to develop, more patient data will be stored within shared care systems. Some of this data will be populated from point-of-care systems automatically. Such data repositories may eventually become the master source of much of a patient’s information.

How can the consumer control their preferences for sharing information? Currently, the population of data into shared care systems and clinical data repositories is controlled by the consumer ‘opting off’ having their information transferred. The problem is that this information is not quickly transferrable if needed in an emergency or where there is a serious threat. A safer solution is to have ‘do not disclose’ provisions built into the shared care system which still give effect to the consumer’s wishes but allows them greater flexibility and immediate control over who accesses their data and when. It also allows access by health providers through a ‘break glass’ mechanism in an emergency and where the patient is unable to give their direct consent.

The ability for an individual to stop the transfer of health information to a shared care system is the way the HealthOne shared care system in the South Island operates. However, in practice, very few people (approximately 0.05 percent) have opted not to have their data transferred – and these preferences change reasonably frequently as individuals change their minds about what data they want shared. This experience supports the view that consumers are better off controlling their own preferences for sharing and disclosing information at the point of care.

Customer preferences should be recorded in the shared care system at enrolment or at initial contact with the health provider, establishing the proximity or relationship between the consumer and health provider and giving them the opportunity to explain how and why the collected information will be held. For example, when a newly pregnant woman registers with her lead maternity carer she can be given an information sheet explaining the process and have the opportunity to put any caveats around the sharing of health information or any health programmes she wants to be enrolled in.

### Requirements

Shared care systems must have the ability to control customer preferences for sharing health information (policy).

### ‘Do not disclose’ option

The consumer has a right to set a ‘do not disclose’ option on sharing some or all of their information. Where this has occurred, the health provider attempting to access the information is notified that some information has been withheld/not disclosed (policy).

### Recommended method of advice

Health providers advise consumers of the risks in a one-on-one conversation (either in person or by phone) before changing consumer’s preferences (policy).

If it is unreasonable in the circumstances to advise consumers face to face or by the consumers’ preferred method of communication, this can be done by other direct communication or through a mass marketing campaign (policy).

* Consumers must be provided with details of who they can contact or how to set their preferences for sharing information in a shared care system (policy).
* Before withholding information, the consumer must be advised of the potential risks in the delivery of care provided to them (policy).

### Enrolment option

Where services are optional, patients will need to enrol and consent to sharing their information on the shared care system (policy).

## Disclosure outside the health and disability sector

Section 22C of the Health Act 1956 says health providers may disclose health information to specific categories of people, on request, if that information is required for those people to carry out their functions. Section 22C, and other relevant legislation under which these requests are likely to be made, are set out in Appendix 10.

Section 22C allows information to be disclosed in response to a request. It does not allow information to be volunteered without a request. Also, the disclosure is always discretionary – the section doesn’t force a heath care provider to disclose.

Some of the categories of people listed in section 22C include police officers, medical officers of penal institutions, probation officers, social workers and care and protection coordinators.

Information may also be disclosed to the employees of a funder (such as a district health board), but only where disclosure of identifiable is essential for carrying out that funder’s functions under the New Zealand Public Health and Disability Act.

### Disclosure to Police and other government or sector agencies

Where a request for personal health information is made, health providers shall check the legal basis for the request. Refer Appendix 10 for the legislation most likely to be cited as the basis for the request (policy).

If the request must be complied with, the health provider shall sight the relevant documents or legislation setting out the third party’s right to require this information before providing it (policy).

Where it is within the health provider’s discretion as to whether or not the information should be disclosed, the health provider shall consider the matter on a case-by-case basis and document their reasons (policy).

### Information matching

Information matching is the comparison of large-scale sets of person records between government departments. An example is the link between primary care enrolment data and immigration data to determine a person’s eligibility for primary health organisation (PHO) funding. In some programmes, it is the absence of a person in one set of records that is of interest. The process is commonly used to determine eligibility for publically funded services.[[44]](#footnote-44). Further information on the rules around information matching can be found in Appendix 11.

### Requirements

Health providers shall only undertake information matching as provided under Part 10 of the Privacy Act 1993 (law).

### Approved Information Sharing Agreement (AISA)

An approved information sharing agreement (AISA) allows information sharing that would otherwise be unlawful between and within agencies to deliver public services. Further detail on AISAs and how they work can be found in Appendix 12.

### Requirements

Health providers may share personal health information only where permitted by the Privacy Act 1993 and Health Information Privacy Code 1994 or by an AISA or other legislation that permits or requires the disclosure of personal health information[[45]](#footnote-45) (law).

## Secondary use of information

The primary use of personal health information by health providers is for treatment and care. However, the data is also often used for secondary purposes such as service management, planning, performance monitoring and funding.

The use of health information for secondary purposes is permissible where the purpose was identified and stated at the point of collection, or where the information is used for research or statistical purposes but not published in a way that identifies the consumer.

For this reason most GPs and DHBs state in documents such as enrolment forms, or privacy fact sheets, a wider list of uses than ‘treatment and care’. Accordingly, where providers propose to use personal health information, they need to ensure their consent forms clearly set out all possible purposes for which the information collected may be used.

It is important to distinguish between personal health information which identifies the individual, and anonymised information in which the individual’s direct identifiers have been removed, as the rules around the sharing of information for each differ. Canterbury District Health Board has provided guidelines on the types of data and degrees of anonymisation which these guidelines have adopted. Further detail on the types and degrees of anonymisation can be found in Appendix 13.

### Requirements

Personal health information shall only be used for secondary purposes:

* with the knowledge of the consumer
* if the use is in line with the original purpose for which the information was collected
* where there is a serious threat to the patient’s safety
* where it is required by law, or
* if it is permitted by an AISA
* where it is to be used for research or statistical purposes but not published in a way that can identify the consumer[[46]](#footnote-46).(law).

Where information is to be analysed in anonymised form the level of anonymisation required is that for de-identified information as set in Appendix 13 (policy)

There is no restriction on the use of anonymised information[[47]](#footnote-47) (law).

Health providers shall not attempt to re-identify the data from which identifying information has been removed unless they have express consent to do so, or it is necessary to prevent or lessen a serious threat to the safety of an individual or public health.

## Access control[[48]](#footnote-48)

### Authorised access

As a guiding principle, health information shall only be accessed by persons who have authorised access and only in the performance of their duties.

* Authorised access means that a higher delegated authority has given permission to an individual employee, contractor or agent to access personal health information in the course of their duties. Authorised access may be direct or indirect.
* Direct authorised access means that authorisation has been given to a named individual by the person to whom the information relates (ie, by informed consent).
* Indirect authorised access is access that has been granted:
* by virtue of the individual user’s role and function (eg, health practitioner, or health service administrator)
* where a person has enrolled in, is registered with, or is admitted to a health service
* in the case of an emergency where the individual is unable to give his/her consent
* where there is a need to prevent or lessen a serious threat[[49]](#footnote-49)
* where the consumer is under 16, and a request has been made by his or her parent/guardian, and disclosure of the information is not against the consumer’s wishes or interests[[50]](#footnote-50)
* by law.
* A person’s authorisation is not necessary where:
* the information is information in general terms concerning the presence, location, and condition and progress of a patient in hospital, on the day on which the information is disclosed, and the disclosure is not contrary to the express request of the individual or his or her representative,[[51]](#footnote-51)or
* de-identified information is being used for the purposes of health statistics or analysis.[[52]](#footnote-52)

### Requirements

Individual users shall be granted access to a system containing personal health information:

* if authorised by a delegated authority
* if required to perform their duties (policy).

## Role-based access control

Role-based access control (RBAC) is a method of regulating access to personal health information based on the role and function of individual users. Software applications can be configured to conform to a RBAC matrix.

Using such a matrix, managers of the system can determine what users can view or change, based on what they know or do. For example, the role of a ‘GP’ would allow access to a shared care system, while the role of a ‘podiatrist’ would have more limited access.

RBAC is reinforced by physical security controls (eg, proximity cards, swipe cards, keys, combination locks on doors).

In all cases for RBAC, gratuitous sharing of the security controls (whether a computer account name and password, proximity cards, swipecards, keys, combination numbers for door locks) is not acceptable as it risks a breakdown in the confidence that both consumers and medical staff place on their safety and privacy.

Proximity also needs to be considered, as part of a circle of care approach, or by proactive auditing. Circle of care explicitly identifies the ‘proximity’ or relationship that a user has to the patient. The combination of RBAC, proximity management, physical security and the code of conduct will provide a ‘defence in depth’ series of conditions for managing legitimate access.

### Requirements

Health care systems require role-based access controls.

Health providers shall implement role-based access for individual users of their systems and undergo systematic security access audits (policy).

Where a person changes a role, their role-based access should be reviewed (spot audit) or where they leave an organisation their access rights are revoked.

RBACs – whether system based or physical – should not simply be passed on to a new person in the same role but should be reissued in the new person’s name. This is particularly true of computer accounts and passwords, proximity cards and swipe cards. Keys should also be handed over and reissued.

Where the health provider has reason to believe there has been inappropriate access of a consumer’s health record, this must be investigated quickly. If there is a suspected breach the consumer shall be advised promptly (policy/law).[[53]](#footnote-53)

## Resource

An example of a RBAC matrix that has been developed by Health One can be found in Appendix 14.

# Securing and protecting personal health information

Personal health information must be held securely to maintain trust and confidence in the health system. Health practitioners accessing the information must be confident it has not been altered by a third party without authorisation, or otherwise compromised. Likewise, consumers must be able to trust that their information is only viewed or updated by those involved in their treatment and care or in accordance with the law.

The requirement to secure health information is covered by the Health Information Security Framework (HISF). Given that, these Guidelines do not re-traverse the same ground but instead refers to the HISF for the requirements in terms of security.

## Objective

Personal health information is protected from unauthorised access or misuse and is maintained securely.

## Policy statements

Health providers must have policies in place to secure health information in transit and in place. They must audit and monitor access, safeguard information from unauthorised access and have security measures to prevent intrusion.

Health providers must have a policy governing retention and disposal of health records. Health information is not held indefinitely and when it is deleted, this must be done securely.

|  |  |
| --- | --- |
| **Relevant Health Information Privacy Code Rules** | |
| Rule 5 | Health providers must ensure there are reasonable safeguards in place to prevent loss, misuse or disclosure of health information. |
| Rule 9 | Health providers can only keep personal health information for as long as is necessary to carry out the purpose for which the agency got the information in the first place. |
| Rule 12 | A health provider cannot use the unique identifier given to a person by another agency (eg, NHI). |

### Requirements

Health providers shall comply with the requirements of the Health Information Security Framework. A copy of the framework can be found at:<http://healthitboard.health.govt.nz/standards/approved-standards/hiso-100292015-health-information-security-framework> (policy).

## Use of cloud or hosted services for managing health information

Cloud computing provides a health care agency with access to large or specialist capacity computing resources not owned by the health care agency but with access being provided across a network. The ‘cloud’ descriptor derives from the non-visible presence of the physical computing location. Access to information for processing and storage is ubiquitous – available anywhere at anytime. The user’s data and application processing sits in the cloud and the user interacts with these services through an internet enabled device. Cloud computing contracts can be established to allow health providers to use the chosen computing resources on a pay-per-use or subscription basis. There is no need to maintain additional processing hardware and software locally.

However, there are risks associated with utilising these services. For example, those of sovereignty when the cloud or hosted service is operated in an overseas location and is therefore outside the jurisdiction of New Zealand law.

### Requirements

All health providers wanting to store personal health information in a cloud environment may do so provided they undertake a risk assessment before doing so and are satisfied with the resulting risk profile. The recommended tool to support the risk assessment remains the GCIO cloud assessment tool (this will be mandatory for DHBs).

DHBs must forward a copy of the completed GCIO risk assessment to the GCIO for their records.

Where the risk assessment identifies areas of concern (red flags) the health provider may wish to discuss the matter with the Ministry of Health (email [cloudcomputing@moh.govt.nz](mailto:cloudcomputing@moh.govt.nz)) before making their decision. Particular areas that may generate concerns are summarised in section 18 of the Health Information Security Framework.[[54]](#footnote-54) They include:

* sovereignty
* governance
* confidentiality
* integrity (of provider)
* availability
* incident response/management.

DHBs are expected to operate an application portfolio management system which covers cloud services as part of its portfolio.

DHBs will report annually to the Ministry identifying what personal health information is held offshore, with which cloud service it is held and in what country or countries.

Government departments and DHBs are also required to have a strategic plan for how they intend to use public cloud services.[[55]](#footnote-55)

### Resources

The Government Chief Information Officer (GCIO) has prepared a risk assessment tool which is a useful starting point in determining risk. While this is voluntary for those outside the public sector (who may choose to use a different risk assessment model), it is mandatory for DHBs and government agencies.

A copy of the risk assessment tool can be found here: https://www.ict.govt.nz/guidance-and-resources/using-cloud-services/assess-the-risks-of-cloud-services/

For further detail on the requirements on government agencies and DHBs on strategic planning and use of the cloud see; https://www.ict.govt.nz/guidance-and-resources/using-cloud-services/

# Governance and implementation of these Guidelines

These Guidelines will be governed by a multi-disciplinary body comprised of health and disability sector representatives, including consumer and clinical representation.

Implementation of these Guidelines will require significant changes in the sector involving both cultural, technical and procedural focus. A communication version for consumers, health practitioners and health executives will be needed. These will reference the full Guidelines for those wanting more detail.

Appendix 1: Compliance checklist

[Data quality](#dataqualitypolicy)

Do your health records comply with the:

* Health (Retention of Health Information) Regulations 1996
* Health Information Privacy Code 1994, rule 9
* governing General Disposal Authority (if applicable).

Is there is a policy in place for managing the coexistence of paper and electronic records?

Does your health information system connect to the NHI and New Zealand Universal List of Medicines?

Does your health information system comply with the Health Information Security Framework?

Can your health information system store ethnicity data at level 4 and hold up to six ethnicities?

[Managing information privacy](#Managinginformationprivacy)

Do you have a designated privacy officer?

Do you have clear policies and procedures covering the collection, use, disclose, storage and access to personal health information? Do you monitor adherence to this policy?

[Code of conduct](#codeofconduct)

Do you have a code of conduct?

[Privacy complaints and breach policy](#privacycomplaintsandbreachofprivacy)

Do you have a policy to manage privacy complaints and breaches of privacy.

[Privacy impact assessment](#privacyimpactassessments)

If you are implementing a new information system have you undertaken a privacy impact assessment?

[Health literacy](#healthliteracy)

Are your communications based on the assumption that the consumer has little health literacy? Have your communications been tested with consumers?

[Information on privacy, patient notification and consent](#informationonprivacypatientnotification)

Do you have available up-to-date and accurate privacy fact sheets? Are these displayed prominently?

[Rights of access and correction](#rightsofaccessandcorrection)

Do you understand the consumer’s rights of access and correction to their health record? In particular, in what circumstances can the parent access their child’s record? In what circumstances can the child refuse the parent access to their record?

[Training and education](#trainingandeducation)

Do you provide training and education to staff on privacy and the appropriate sharing of data?

[Audit logs](#auditlogsandproximity)

Does your clinical information system have an audit log?

Do you review the audit log a minimum of monthly and investigate all apparent outliers and break glass accesses?

[Patient portal](#patientportals)

Do you have a patient portal?

Does it comply with the HISO 10029 Health Information Security Framework <http://ithealthboard.health.nz/hiso-10029-health-information-security-framework>?

Do you have a policy in place on staff access to shared care systems?

[Consumer preferences for sharing information](#consumerpreferences)

If you are transferring patient information into a shared care system have you taken steps to advise the patient that this has occurred and of their rights in respect of this?

If consumer information is being included in a Shared Care System, what controls do consumers have over the sharing of their health information?

[Disclosure to policy and other government of sector agencies](#disclosureoutsidehanddsection)

If you receive a request for disclosure of identifiable information by a third party have you checked the legal basis for the request? (Refer Appendix 10 for the legislation most likely to be cited as the basis for the request.)

[Approved Information Sharing Agreement (AISA)](#aisa)

Is the sharing covered by an AISA or other legislation that permits or requires the disclosure of personal health information.[[56]](#footnote-56) What are these?

[Secondary use of information](#secondaryuseofinformation)

If you are using personal health information for secondary purposes:

* does the consumer know
* is the use is in line with the original purpose for which the information was collected
* is there a serious threat to the patient’s safety
* is it required by law, or
* is it to be used for research or statistical purposes but not published in a way that can identify the consumer?[[57]](#footnote-57)

What safeguards do you have in place to prevent the re-identification of anonymised data used for analytical or statistical purposes?

[Authorised access](#authorisedaccess)

How do you authorise access by users to your systems? What safeguards to you have in place to prevent or monitor unauthorised access?

[Role-based access control](#rbac)

Have you implemented role based access control for your electronic health record system?

Are you following up in situations where there appears to have been inappropriate access to a consumer’s health record?

[Securing and protecting personal health information](#securingandprotectingpersonalhealthinfo)

As a health provider are you compliant with the Health Information Security Framework. A copy of the Framework can be found at (<http://healthitboard.health.govt.nz/standards/approved-standards/hiso-100292015-health-information-security-framework>).

[Use of cloud or hosted services for managing health information](#useofcloud)

Are you storing personal health information overseas? If so have you undertaken a risk assessment of the proposed product or service?

If you are a DHB or government agency, have you complied with the GCIO’s requirements in respect of strategic planning?

Appendix 2: Relevant legislation

Privacy Act 1993 and Health Information Privacy Code 1994

The Privacy Act 1993 regulates the collection, disclosure and use of personal information in New Zealand by way of 12 information privacy principles. The Privacy Commissioner, an Independent Crown Entity, administers the Act’s complaints and information sharing provisions. The Commissioner is also able to create codes to regulate specific sectors where necessary.

The Health Information Privacy Code 1994 is a code created by the Privacy Commissioner under the Act to regulate health information. It applies to all health and disability service providers in the public and private sectors. The Code consists of 12 health information privacy rules, as well as setting out which agencies are allowed to assign the National Health Index number, who may charge a fee for providing an person with access to their own health information, and the rules around how health agencies should deal with patient complaints. The 12 health information privacy rules can be summarised from the perspective of the health practitioner as follows:

1. Only collect health information if you really need it.

2. Get it straight from the people concerned, where possible.

3. Tell consumers what you’re going to do with it.

4. Be considerate when you’re getting it.

5. Take care of it once you’ve got it.

6. People can see their health information if they want to.

7. They can correct it if it’s wrong.

8. Make sure health information is correct before you use it.

9. Get rid of it when you’re done with it, if the law allows.

10. Use it for the purpose you got it.

11. Only disclose it if you have a good reason.

12. Only assign unique identifiers where permitted.

While this list is a useful overview and starting point, most of the rules have exceptions and anyone dealing with health information should at least have read the 12 rules in full.[[58]](#footnote-58)

Some useful points to note about the 12 health information privacy rules:

* Rule 2 requires health agencies collecting external electronic health records to get permission from the consumer to do so where practicable (such as in a face to face consult)
* Rule 3 requires health agencies to carefully consider how purposes and intended uses/disclosures are being explained to their patients, for instance by verbal discussions, posters, brochures and admission forms.
* Rule 7 allows patients to seek correction of health information they disagree with, but doesn’t require agencies to make the correction sought. However it does require health agencies to attach a statement from the patient to the record on request, setting out the correction sought but not made.
* Rule 9 is affected by laws requiring health record retention which take precedence over it; the minimum retention period of health records is 10 years since the last consult.[[59]](#footnote-59)
* Rule 11 allows disclosure in a number of common situations specific to the health sector (presence, location and condition in hospital, talking to relatives, and disclosure of serious threat to someone who can help prevent or lessen the threat) and should be studied carefully.

The Privacy Act and the Health Information Privacy Code are both subject to any other legislation that requires or allows disclosure of information. Other key pieces of legislation are listed below.

Official Information Act 1982

Requires any public sector organisation to supply information on request, except where releasing the information would breach someone’s privacy.[[60]](#footnote-60)

Health Act 1956

* Allows (but does not require) health agencies to disclose health information, on request, to specified official agencies such as the Police.[[61]](#footnote-61)
* Requires health agencies to disclose health information about a patient, on request, to people providing health care to that patient or representatives of the patient, unless responding to the request would be against the wishes or interests of the patient.[[62]](#footnote-62)
* Allows anonymised health information to be shared without the need to obtain the consent of the consumer or consumers to whom the information relates.[[63]](#footnote-63)

Oranga Tamariki Act 1989 Children’s and Young People’s Welfare Act 1989[[64]](#footnote-64) (previously Children, Young Persons, and Their Families Act 1989)

This Act permits disclosure of any information suggesting that a child or young person is being or might be abused or deprived in any way, to a social worker or the Police.[[65]](#footnote-65)

An amendment to this Act will come into force on a date appointed by Order in Council or by 1 July 2019 if it has not earlier been brought into force. This amendment will provide for an information sharing framework that facilitates the timely and consistent exchange of information about vulnerable children and young people to promote their safety and wellbeing. The framework:

* includes a presumption that when information is requested for child welfare and protection purposes it will be shared
* allows linked data-sets of information sourced from multiple agencies to be analysed for operational purposes, and to inform risk and needs assessment, service design and delivery.[[66]](#footnote-66)

HDC Code of Health and Disability Services Consumers’ Rights Regulation 1996

Establishes the rights of consumers, and the obligations and duties of providers to comply with the Code. In particular:

i. consumers have the right to be fully informed about any diagnosis given, as well as the options available in respect of treatment and care (Right 6), and the right to make an informed choice or give informed consent to any treatment and or care proposed (Right 7)

ii. a full list of all relevant legislation can be found in the appendix to the HIPC 1994 Commentary <http://privacy.org.nz/assets/Files/Codes-of-Practice-materials/HIPC-1994-incl.-amendments-revised-commentary.pdf>.

Appendix 3: Definitions

Definitions

Agency

Agency in terms of the Health Information Privacy Code, means an agency referred to in clause 4(2) (of the Code) and, is to be taken to include, –

a) where an agency holds health information obtained in the course of providing health or disability services but no longer provides such services, that agency; and

b) with respect to any health information held by a health agency (being a natural person) at the time of the person’s death, his or her personal.

Clause 4(2) provides further detail on types or classes of agency and includes health and disability service providers.

Authorised access

Authorised access means that permission has been given to an individual to access personal health information. Authorised access may be direct or indirect.

Direct authorised access means that authorisation has been given to a named individual by the person to whom the information relates (ie, by informed consent).

Indirect authorised access is access that has been granted:

* by virtue of the individual’s role and function (eg, doctor, nurse or health service administrator)
* in the case of an emergency where the individual is unable to give his/her consent
* where there is a need to prevent or lessen a serious threat
* by law.

Cloud computing

The New Zealand Cloud Computing Code of Practice[[67]](#footnote-67) defines cloud computing as “on-demand scalable resources such as networks, servers and applications which are provided as a service, are accessible by the end user and can be rapidly provisioned and released with minimal effort or service provider intervention”.

Confidentiality

Pertains to the treatment of information that an individual has disclosed in a relationship of trust and with the expectation that it will not be divulged to others in ways that are inconsistent with the understanding of the original disclosure, without permission.

Consumer

A consumer is someone who has used, is using or will use health care services. The words ‘consumer’ and ‘patient’ are synonyms for the purposes of this document.

Custodian of health information

A custodian of health information is a person or an organisation that holds health information for the purpose of providing health care services. In collaboration with the consumer (and in accordance with the law), the custodian controls access rights to and disclosure of that information. They are required by law to maintain confidentiality and security over the health information they hold. A custodian may also be an infrastructure provider, however, the two roles are not the same.

Data quality

The dimensions of high data quality are that the information is:

a) complete (in terms of having been captured in full)

b) accurate (the proximity of the data to the exact or true values)

c) relevant (the degree to which the data meets current and potential user’s needs)

d) accessible (data must be retrievable in order to be used and in order to assess its quality)

e) timely (recorded and available as soon after the event as possible)

f) valid (within an agreed formal which conforms to recognised national standards)

g) defined (understood by all staff who need to know, and is reflected in procedural standards)

h) appropriately sought (in terms of being collected or checked only once during a period of care)

i) appropriately recorded (in both paper and electronic records).

Electronic health record

An electronic health record (EHR) is a longitudinal shared care health record of patient information generated by encounters with health providers and which is stored and retrievable through electronic means.

Health agency

A health agency is an organisation that is in the business of providing health care services to the health and disability sector.[[68]](#footnote-68)

Health provider

A health provider means any person or organisation involved either directly or indirectly in the provision of health care and includes a health agency. There are two kinds of health provider persons: a health practitioner and a health care worker.

Health practitioner

A person who is, or is deemed to be, registered with an authority established or continued by section 114 of the Health Practitioners Competence Assurance Act 2003, as a practitioner of a particular health profession.

Health care worker

A person not registered with a Responsible Authority who provides a health care related service within the health and disability sector. Examples include:

* a social worker
* an acupuncturist
* a clinical coder
* an auditor working in the health field
* an administrator or receptionist working in a DHB, general practice or other health agency.

Health information/personal health information

Health information is defined, broadly, in clause 4 of the Health Information Privacy Code 1994 and includes any information about the health of an identifiable individual, or any health or disability services provided to him or her. It also includes any information collected incidentally to providing services, such as appointment times and demographic data. It does not include anonymous data as it must be about an identifiable individual.

This document focuses on the sharing of health information as defined above. For clarification, we have referred to any information about the health of an identifiable individual as personal health information.

Health Information Privacy Code 1994 (HIPC)

Health Information Privacy Code 1994 (HIPC): The HIPC is a code of practice issued by the Privacy Commissioner that modifies the 12 information privacy principles of the Privacy Act into 12 information privacy rules. The HIPC rules are generally similar to the principles they are modelled on, but are tailored for the health sector’s needs. A copy of the code can be found at <http://privacy.org.nz/assets/Files/Codes-of-Practice-materials/HIPC-1994-incl.-amendments-revised-commentary.pdf>

Health record

The health record is essentially a record describing every aspect of the health care provided to an identifiable consumer/patient and may be in a single file, multiple file, hard copy (paper-based) or electronic (digital, audio, video, etc) format, and held by a health provider or the consumer/ patient themselves.

Components of a health record may include information in relation to the consumer’s or patient’s:

* assessment
* investigations and results
* diagnosis
* plan of care
* prevention and health promotion activities
* Treatments, medications and procedures provided
* consumer/patient progress
* health and support services provided
* evaluation and review of service provided
* follow-up and ongoing care/treatment.[[69]](#footnote-69)

Infrastructure provider

The person or organisation responsible for providing the servers, data networks and operating environment that support the information service. For example, an infrastructure provider may provide the health agency with some or all of the following:

* computing hardware and power/cooling (usually within a data centre operated by the infrastructure provider)
* virtual machine, operating system and system management software
* network connectivity
* online disk storage
* offsite and archive storage capacity.

Interface

An interface enables the transfer of structured information between two systems.

Opt on/opt off

The process by which a consumer’s personal health information is included on a shared care system.

Opt on

The consumer is required to give their explicit consent before a copy of their information is transferred into another system.

Opt off

The consumer is informed that a copy of their information is to be transferred to the system unless they specifically decide not to transfer their information. If the latter is the case they will be marked as ‘opt off’.

Point of care

See shared care.

Portals

Portals are a secure, web-based application that brings together information from one or more sources, presents information to the user in a consistent way, and has access control. A consumer may have a portal interface into their patient notes held on the GP’s system, or, if their GP has included the consumer’s patient notes in a shared care system, then they may have a view of the information held in that.

Similarly, there are also clinical portals that allow health practitioners access to patient notes. Such access is limited and whether the health practitioner can access the notes will depend on their role and function and that the consumer/patient has not chosen to withhold the information.

As well as clinical portals in DHBs, access to a patient’s notes is controlled through a clinical work station. A clinical workstation is also a secure web based application and is used by health practitioners to access and update information held in the electronic health record.

Representative

Representative is defined in the Health Information Privacy Code 1994. In relation to an individual, representative means where:

a) that individual is dead, that individual’s personal representative, or

b) the individual is under the age of 16 years, that individual’s parent or guardian, or

c) the individual, not being an individual referred to in paragraphs a) or b), is unable to give his or her consent or authority, or exercise his or her rights, a person appearing to be lawfully acting on the individual’s behalf or in his or her interests.[[70]](#footnote-70)

A person appearing to be acting contrary to the interests of the individual would not be regarded as an individual’s representative under paragraph c) above.

Role-based access control

Role-based access control (RBAC) is a method of regulating access to personal health information based on the role and function of individual users within a health agency. Using the Role Based Access Control Matrix, managers of the system can determine which health practitioner should have access to which types of records. What they can view will depend on what they need to know for the purposes of their role and function. For example, A RBAC matrix in the health system would normally show that a GP has access to most of the single EHR while the access for a community podiatrist will be more limited.

Serious threat

Serious threat is defined in section 2 of the Privacy Act 1993, and means a threat that is serious, on balance, because of its imminence, its potential severity and its likelihood. Where it is necessary to prevent or lessen a serious threat, some privacy protections can be overridden.

Shared care (also covers Point of care)

Health information can be accessed in point of care systems or shared care systems. On paper the two types of system seem quite different.

For example, a point of care electronic health record system is a system which the consumer’s health practitioner uses to manage their Health Record at the point of care (ie, the point where there is direct communication and interaction between the consumer and the health practitioner). Under this model the information is typically not shared with other health providers.

A shared care system by contrast may contain either a partial or complete record of the consumer’s health information held electronically that can be made available to and shared with different health providers and the consumer themselves. It typically takes its source data from point of care clinical information systems used by health practitioners to maintain the patient’s health record (see Point of care).

In practical terms, however, the distinction between point-of-care systems and shared care systems is not always clear as a point of care systems have limited shared care functions and shared care systems have limited point of care functions.

For example in a hospital setting a clinical portal system might be used by different people as either a point of care or shared care system depending on what their role and function is in relation to the patient. For example, a typical point of care function in a clinical portal is the creation of a discharge summary.

In a general practice, the GP’s practice management system is typically thought of as a point of care system but also possesses aspects of being a shared care system. Typically, not only will the treating general practitioner be able to see the patient’s personal health information but so will other general practitioners in the practice, the practice nurse and limited information will also be made available to the receptionist/administrator for the purpose of booking appointments.

It would be more accurate to think of EHR systems as sitting on a continuum, with point of care systems situated at one end and shared care at the other. Where along the continuum a particular system is will depend on how many people have access to it.

User

A user is a person issued with a unique user ID who is authorised to use a computer system.

Appendix 4: Key information governance principles

This appendix documents the key principles on which these Health Information Governance Guidelines are based.

Consumers and patients expect that personal health information provided to their health providers will be kept confidential. They must feel able to share sensitive information with a health practitioner without fear that the information will be improperly disclosed. Health services cannot work effectively without trust and trust depends on confidentiality.

However, consumers and patients also expect health practitioners to share clinical information with other members of the care team. Health information may also be disclosed for legally supported purposes.[[71]](#footnote-71) To support a seamless experience for the consumer, information needs to be available to health providers at the right place and the right time. Safe sharing of information through point-of-care or shared care systems is as important as maintaining confidentiality. Health providers must succeed in both respecting confidentiality of information and sharing it appropriately.

Our health system continues to demand higher levels of integration to ensure improved quality and productivity. In response to this demand, health practitioners have increased their use of technology to share the information they need with each other. While this makes sharing health information easier and more reliable, attention must be given to ensuring that consumer and health provider trust in systems is maintained.[[72]](#footnote-72), [[73]](#footnote-73)

In drafting these Guidelines HIGEAG first developed a set of general principles governing the use of personal health information. These principles draw on the Health information Privacy Code 1994 as well as the Code of Health and Disability Services Consumers’ Rights and the document “Protecting Personal Health Information – Consumer Expectations” prepared by the Ministry’s Technology and Digital Services’ Consumer Panel.

Quality and trust

High quality health information supports high quality health care. This means:

* consumers trust that the health system will keep their information safe
* information is available to inform any health care decision related to that consumer
* information held is as accurate, up to date and relevant as is necessary for the purposes of treatment and care.

Maintaining trust between consumers and health agencies requires the safe sharing of health information. This means:

* all health information is treated as confidential
* health information is held securely and in accordance with national standards
* health information is only accessed by persons who have authorised access and only in the performance of their duties
* health information remains under the jurisdiction of the health and disability sector unless authorised by law or the consumer has explicitly given their permission
* custodians of health information protect it against loss and unauthorised access, use, modification or disclosure.

Privacy and transparency

On the collection of health information, health agencies will communicate the likely intended purpose and disclosures of the information to the consumer in a straightforward way.

A consumer has a right to access and take a copy of their health information and to know who else has accessed it. They do not need to give a reason for requesting that information.

A consumer has the right to ask for their health information to be corrected. If their request is refused a consumer has the right to have a note added to their records listing any correction sought but not made.

Consumers may withhold from sharing part, or all, of any of their health information that is not required to be disclosed by law. This means:

* before a consumer chooses to withhold information, their health practitioner will advise them if it could affect the quality of health care and treatment provided, and/or could pose risks to their health
* where information is withheld a notation will be made on the health record indicating that this has occurred.

Disclosure

A health agency may use or disclose a consumer’s health information if they have been granted Authorised access to do so or for purposes that have been communicated to the consumer. Likely purposes for disclosure include: delivery of care, referrals, research, teaching, audit and funding.

Where permitted by law, health information may be disclosed without the consumer’s permission. For instance when the:

a) consumer is unconscious or otherwise unable to give permission and disclosure is necessary for the purposes of treatment

b) consumer refuses to give permission but the information is necessary to prevent or lessen a serious threat

c) consumer is under 16, a request has been made by his or her parent/guardian, and disclosure of the information is not against the consumer’s wishes or interests

d) consumer is in hospital, has not asked for his or her presence to be kept secret, and the information being disclosed about the consumer is only their presence, location and condition[[74]](#footnote-74)

e) only anonymous information is being disclosed.[[75]](#footnote-75)

Security

Health agencies must establish reasonable safeguards to monitor and protect health information – refer HISO 10029:2015 Health Information Security Framework[[76]](#footnote-76).

The safeguards should provide for:

a) clear identification of the parties involved in any health care transaction, including the consumer, the health provider person(s) and the health agency

b) event auditing and security alerts

c) governance processes to respond to privacy complaints and security breaches

d) ongoing user security training

e) proper procedures to grant authorisation to people to access the data

f) compliance with the Health Information Security Framework and role-based access control.

Data networks that handle health information must be resilient against intrusion, negligence and accidental damage including data corruption and loss.

Health information is not held indefinitely and when it is deleted this must be done securely.

Appendix 5: Privacy access escalation ladder

The escalation ladder

Sharing information involves both the collection and disclosure of personal information. Deciding which laws apply and what information to share can be complicated, but there are some guiding rules.

How to use the escalation ladder

Work through from question 1 to question 5 and stop when you can answer ‘yes’.

If the answer to all of the five questions is ‘no’, then disclosure should be unnecessary and should be avoided, at least for now.

Remember that the proportionality principle always applies – you should only provide as much information as is reasonably necessary to achieve your objectives.

Question 1: Can we get by without naming names?

* Use anonymous information where practical.
* Disclosing anonymous information is always okay. (For example, if you have professional supervision, you might be able to discuss a case without referring to any names.)

Question 2: Have they agreed?

* If information is not able to be used anonymously, the best thing is consent from the parties concerned.
* Consent does not need to be written.
* Always record the fact that parties have agreed. Record any limitation or qualification of consent, eg, “please don’t involve the church”.

Question 3: Have we told them?

* If it is not practicable or desirable to obtain consent, the information may be used or disclosed if it is in line with the purpose for which it was obtained.
* Inform the person affected of this where possible – ideally at the time the information was first collected from them, or soon after that.
* If informing the person would prejudice the purpose of collection, or would be dangerous to any person, then telling the person concerned may be waived in that instance.

Question 4: Is there a serious threat

Information may be used or disclosed where there is a serious threat.

What is considered serious depends on:

* how soon the threatened event might take place
* how likely it is to occur
* how bad the consequences of the threat eventuating would be.

Question 5: Is there another legal provision we can use?

Many different laws allow personal information to be shared. For instance, health information:

* about the health/safety of a child or young person can always be disclosed to a police officer or social worker
* can be requested by someone who needs it to provide health services
* can be disclosed where necessary to avoid prejudice to the maintenance of the law
* can be shared under an AISA.

If the answer to all of the five questions is ‘no’, then disclosure should be unnecessary, and should be avoided, at least for now.

Appendix 6: Privacy fact sheet

Use and confidentiality of your health information (fact sheet)

Your privacy and confidentiality will be fully respected. This fact sheet sets out why we collect your information and how that information will be used.

Purpose

We collect your health information to provide a record of care. This helps you receive quality treatment and care when you need it.

We also collect your health information to help:

* help you manage your own health
* keep you and others safe
* plan and fund health services
* carry out authorised research
* train health care professionals
* prepare and publish statistics
* improve government services.

Confidentiality and information sharing

Your privacy and the confidentiality of your information is really important to us.

* Your health practitioner will record relevant information from your consultation in your notes.
* Your health information will be shared with others involved in your health care and with other agencies with your consent, or if authorised by law.
* You don’t have to share your health information, however, withholding it may affect the quality of care you receive. Talk to your health practitioner if you have any concerns.
* You have the right to know where your information is kept, who has access rights, and, if the system has audit log capability, who has viewed or updated your information.
* Your information will be kept securely to prevent unauthorised access.

Information quality

We’re required to keep your information accurate, up to date and relevant for your treatment and care.

Right to access and correct

You have the right to access and correct your health information.

* You have the right to see and request a copy of your health information. You don’t have to explain why you’re requesting that information, but may be required to provide proof of your identity. If you request a second copy of that information within 12 months, you may have to pay an administration fee.
* You can ask for health information about you to be corrected. Practice staff should provide you with reasonable assistance. If your health provider chooses not to change that information, you can have this noted on your file.

Many practices now offer a patient portal, which allows you to view some of your practice health records online. Ask your practice if they’re offering a portal so you can register.

Use of your health information

Below are some examples of how your health information is used.

* If your practice is contracted to a primary health organisation (PHO), the PHO may use your information for clinical and administrative purposes including obtaining subsidised funding for you.
* Your district health board (DHB) uses your information to provide treatment and care, and to improve the quality of its services.
* A clinical audit may be conducted by a qualified health practitioner to review the quality of services provided to you. They may also view health records if the audit involves checking on health matters.
* When you choose to register in a health programme (eg, immunisation or breast screening), relevant information may be shared with other health agencies.
* The Ministry of Health uses your demographic information to assign a unique number to you on the National Health Index (NHI). This NHI number will help identify you when you use health services.
* The Ministry of Health holds health information to measure how well health services are delivered and to plan and fund future health services. Auditors may occasionally conduct financial audits of your health practitioner. The auditors may review your records and may contact you to check that you received those services.
* Notification of births and deaths to the Births, Deaths and Marriages register may be performed electronically to streamline a person’s interactions with government.

Research

Your health information may be used in research approved by an ethics committee or when it has had identifying details removed.

* Research which may directly or indirectly identify you can only be published if the researcher has previously obtained your consent and the study has received ethics approval.
* Under the law, you are not required to give consent to the use of your health information if it’s for unpublished research or statistical purposes, or if it’s published in a way that doesn’t identify you.

Complaints

It’s okay to complain if you’re not happy with the way your health information is collected or used.

Talk to your health provider in the first instance. If you are still unhappy with the response you can call the Office of the Privacy Commissioner toll-free on 0800 803 909, as they can investigate this further.

For further information

Visit [www.legislation.govt.nz](http://www.legislation.govt.nz) to access the Health Act 1956, Official Information Act 1982 and Privacy Act 1993.

The Health Information Privacy Code 1994 is available at [www.privacy.org.nz](http://www.privacy.org.nz). You can also use the Privacy Commissioner’s [Ask Us](https://privacy.org.nz/further-resources/knowledge-base/) tool for privacy queries.

A copy of the Health and Disability Committee’s Standard Operating procedures can be found at <http://ethics.health.govt.nz/operating-procedures>

Further detail in regard to the matters discussed in this Fact Sheet can be found on the Ministry of Health website at http://www.health.govt.nz/your-health/services-and-support/health-care-services/sharing-your-health-information

Appendix 7: Privacy poster

Collecting information about your health

We collect information about your health to help us provide you with the best health care for you.

The information we collect about your health can also help us improve the health services we provide. We use it, and information about other people’s health, to help us:

* work out what are the health services that people need and arrange funding for these services
* train health care professionals in areas of health care that need more services
* arrange for research in areas of health that are of specific concern.

Who can access the health information we collect

All the health information we collect is completely confidential. It is kept in a secure place to prevent unauthorised access.

* We will share your health information with the health professionals who are involved in your health care.
* We may share your information with other agencies with your consent, or if authorised by law.
* We may allow it to be used in health research that has been approved by an ethics committee, or when the information is made anonymous so that no one will be able to link it to you.

Your rights

You have the right to:

* know where your health information is kept
* know who has viewed or changed your information
* see all the health information we collect about you
* ask for changes to be made to your health information or have a note added to your file outlining the change you requested if that change is not made
* stop your health information from being used in certain circumstances.

Complaints

If you want to make a complaint about the collection of your health information, talk to your health provider or the Office of the Privacy Commissioner through their website: www.privacy.org.nz/about-us/contact/ or on freephone: 0800 803 909.

Appendix 8: Code of conduct to safeguard the privacy and confidentiality of patient health information

Confidentiality

There is a responsibility for confidentiality on any person involved in the use and management of health and organisational information. Confidentiality implies that those obtaining health information disclose only what is necessary in order to perform their role in delivering safe health care. This is formalised through employment contracts, non-disclosure agreements, service contracts, and professional ethical guidelines.

Privacy

There is a responsibility to respect an individual’s rights to exercise control over his or her personal information. The Privacy Act guides the amount of control an individual has with respect to collection, storage, use and disclosure of personal information, the right of access to and the right to request correction of personal information.

Health Information Privacy Code (HIPC)

HIPC provides further guidance in relation to the application of the Privacy Act to patient’s health information. In brief:

* only collect health information if you really need it
* get it straight from the people concerned where possible
* tell them what you’re going to do with it
* be considerate when you’re getting it
* take care of it once you’ve got it
* people can see their health information if they want to
* they can correct it if it’s wrong
* make sure health information is correct before you use it
* get rid of it when you’re done with it
* use it for the purpose you got it
* only disclose it if you have a good reason
* only assign unique identifiers where permitted.

HealthSafe Framework

The *HealthSafe Framework* applies the following to the use and management of information:

1. a request and approval process must be followed before users access information stored in a database

2. information obtained must only be used for the approved purpose(s)

3. non-identifiable information should be used whenever this is sufficient for purpose

4. information obtained must not be shared beyond those specifically granted access through the user data request process

5. users must securely transfer, store and dispose of information obtained

6. de-identified information must not be re-identified except where this is permitted through the purpose-use matrix and an approved user data request

7. patient information which is flagged as sensitive in the source system should not be stored or made available in identifiable form

8. anyone who detects a privacy breach must immediately notify a manager or their organisational privacy officer

9. only aggregate or non-identifiable information may be published without obtaining explicit patient consent and this must be approved through user and source data requests.

Appendix 9: Privacy impact assessments

What are the benefits of a PIA?

PIA offers a tool to undertake the systematic analysis of privacy issues arising from a project in order to inform decision-makers. PIA can provide a credible source of information by assuaging alarmist fears or alerting the complacent to potential pitfalls.

In some cases bitter consumer and public reaction has led to the withdrawal of a new and expensively developed product for privacy reasons. PIA ensures that a business is the first to find out about privacy pitfalls in its project, rather than learning of them from critics or competitors. A privacy impact report can save money and protect reputation.

PIA brings privacy responsibility clearly back to the proponent of a proposal. They must ‘own’ any problems and devise appropriate responses in the design and planning phases. It also ensures that divisions within larger businesses recognise that their projects must not jeopardise the trust vested in the wider business.

PIA encourages cost-effective solutions, since it is cheaper to do things at the design phase to meet privacy concerns than attempt to retrofit after a system is operational.

PIA can make the difference between an invasive and a privacy enhancing initiative, without compromising business objectives or adding significant costs.

The Privacy Commissioner can add value to the process by reviewing a privacy impact report, rather than having to investigate the practices of the business itself. This is cost effective for the Commissioner and less intrusive for a business.

Significant risks to privacy exist in e-commerce and e-government. These risks must be confronted if trust and confidence are to prevail in the relationships with consumers and citizens. Until the hallmarks of trust and confidence are reflected in community perceptions, electronic service delivery will be impeded in realising its full potential.[[77]](#footnote-77)

When to undertake a PIA

A PIA should be undertaken as part of the planning stage and once a decision as to what the proposed new system will look like has been determined. This allows privacy issues to be identified and addressed systematically and reliably throughout the life of the project.

Early attention to privacy issues allows for privacy friendly approaches to be considered and implemented which might not otherwise be considered. In the long term, taking privacy seriously helps build people’s trust in government and avoids bad publicity and reduces public resistance to compliance.

Set out below in diagrammatic format is a decision tree for when a PIA is needed. It should not however, be read as an exhaustive list.[[78]](#footnote-78)



Resources

New Zealand

*Privacy Impact Assessment Handbook*, Office of the Privacy Commissioner, 16 July 2008 <http://www.privacy.org.nz/news-and-publications/guidance-notes/privacy-impact-assessment-handbook/>

The Commissioner’s website also has many other helpful resources including explanations of the 12 Privacy Principles <http://www.privacy.org.nz/the-privacy-act-and-codes/privacy-principles/>

The Government Chief Privacy Officer – the office has some useful resources in terms of PIAs. Their contact details are: <https://ict.govt.nz/governance-and-leadership/the-gcio-team/government-chief-privacy-officer/> email: [gcpo@dia.govt.nz](mailto:gcpo@dia.govt.nz)

Australia

#### Office of the Australian Information Commissioner

*Guide to undertaking privacy impact assessments*, May 2014 <http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/guide-to-undertaking-privacy-impact-assessments>

*Guide to undertaking privacy impact assessments – summary*, May 2014 <http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/pia-guide-qrt>

#### Office of the Victorian Privacy Commissioner

Privacy impact assessments guide, April 2009. This page also provides a report template and a guide for completing it. The guide to the template provides an extensive list of common risks and possible mitigation strategies.

https://www.cpdp.vic.gov.au/menu-resources/resources-privacy/resources-privacy-guidelines

A short *Identifying privacy issues early checklist* is available here https://www.cpdp.vic.gov.au/menu-resources/resources-privacy/resources-privacy-link-library

Canada

Office of the Privacy Commissioner of Canada publishes a fact sheet on *Privacy Impact Assessments* https://www.priv.gc.ca/en/privacy-topics/privacy-impact-assessments/

They also have a video *Why think about privacy: A guide to the Privacy impact assessment process*, https://www.priv.gc.ca/en/privacy-topics/privacy-impact-assessments/pia\_2013\_index/

Note: this advice is tailored to a Treasury Board of Canada *Directive on Privacy Impact Assessment* that requires federal government agencies to carry out PIAs that are reviewed by the OPC.

Information and Privacy Commissioner of Ontario, Privacy by Design website. This website has an extensive collection of material about incorporating privacy sensitivity into the design of business processes and supporting computer systems. <http://www.privacybydesign.ca/>

Government of British Columbia

Government agencies are required to conduct PIAs for ‘all new and existing enactments, systems, programs, projects and activities’. This is the page with their PIA *Guidelines* document: <http://www.cio.gov.bc.ca/cio/priv_leg/foippa/pia/pia_index.page>?

United Kingdom

Information Commissioner’s *Conducting privacy impact assessments code of practice* and links to research commissioned for the Office into PIA best practice are available here: <http://ico.org.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment>

United States

The Federal Office of Management and Budget has issued requirements and guidance on PIAs. *M-03-22 OMB guidance for implementing the privacy provisions of the E-Government Act of 2002.* https://www.whitehouse.gov/omb/information-for-agencies/memoranda#memoranda-2002

*Model privacy impact assessment for agency use of third-party website and applications* <http://www.whitehouse.gov/sites/default/files/omb/inforeg/info_policy/model-pia-agency-use-third-party-websites-and-applications.pdf>

Other material can be found through this page: <http://www.whitehouse.gov/omb/inforeg_infopoltech/#pg>

The National Institute of Standards and Technology publishes *Security and privacy controls for federal information systems* NIST-SP 800-53, Revision 4. Appendix J contains the privacy controls (risk mitigations). <http://www.nist.gov/manuscript-publication-search.cfm?pub_id=915447>

Appendix 10: Disclosure to third parties

Disclosure to Police and other government or sector agencies

Requests for disclosure of identifiable health information official agencies like ACC, the Ministry of Health or the Police can raise dilemmas for health agencies; on the one hand, every health agency needs to respect the confidentiality of the patient; on the other hand there are a number of laws that either allow or (rarely) require information to be disclosed.

The first question to resolve is whether the disclosure is compulsory, and what will happen if the request for disclosure is refused. Asking for the legal basis of the decision (a copy of the search warrant or reference to the applicable legislation) is good standard practice. Some of the few agencies that can require information to be provided are:

Section 11 of the Social Security Act 1964

Where the Ministry of Social Development needs to –

* determine whether a person is receiving, or has received, or made a claim for, a benefit or payment under the Social Security Act or related legislation
* determine the rate of benefit or payment that is or was applicable to that person; or
* determine whether a person who has been issued with, or has made a claim for, an entitlement card under regulations in force is or was entitled to be issued with that card; or
* conduct or review a means assessment relating to payment for contracted care services
* determine the amount that any person is required to pay towards the cost of home-based disability support services supplied to that person, and whether a person who has been so assessed is entitled to that assessment; or
* ascertain the financial circumstances or whereabouts of any person who is indebted to the Crown under this Act or related legislation
* discharge the chief executive’s functions under Social Security Act or its regulations –

it may request any person to provide the Ministry of Social Development with any information it requires.[[79]](#footnote-79)

The request must be made by notice in writing and must comply with the Code of Conduct for Obtaining Information under section 11 of the Social Security Act 1964.[[80]](#footnote-80)

Advice from another health provider that it is or is going to be providing health care to the individual concerned under section 22F of the Health Act

Section 22F provides:

(1) Every person who holds health information of any kind shall, at the request of the individual about whom the information is held, their representative or any other person that is providing, or is to provide services to that individual, disclose that information to that individual or, their representative or to that other person.

(2) A person that holds health information may refuse to disclose that information under this section if —

(a) that person has a lawful excuse for not disclosing that information; or

(b) the information is requested by someone other than the individual about whom it is held (not being a representative of that individual) and the holder of the information has reasonable grounds for believing that that individual does not wish the information to be disclosed; or

(c) refusal is authorised by a code of practice issued under [section 46](http://www.legislation.govt.nz/act/public/1956/0065/latest/link.aspx?id=DLM297408) of the Privacy Act 1993.

(3) For the purposes of subsection (2) (a), neither –

(a) the fact that any payment due to the holder of any information or to any other person has not been made; nor

(b) the need to avoid prejudice to the commercial position of the holder of any information or of any other person; nor

(c) the fact that disclosure is not permitted under any of the information privacy principles set out in [section 6](http://www.legislation.govt.nz/act/public/1956/0065/latest/link.aspx?id=DLM297038) of the Privacy Act 1993 –

shall constitute a lawful excuse for not disclosing information under this section.

(4) Where any person refuses to disclose health information in response to a request made under this section, the person whose request is refused may make a complaint to the Privacy Commissioner.[[81]](#footnote-81)

The Minister of Health under section 22D of the Health Act (only applies to DHBs)

Section 22 D provides:

(1) 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.

(2) Subject to subsection (3), it is the duty of a district health board to provide the returns or other information specified in a notice given to it under subsection (1) within such time, and in such form, as is specified in the notice.

(3) No information that would enable the identification of an individual may be provided under this section unless –

(a) the individual consents to the provision of such information; or

(b) the identifying information is essential for the purposes for which the information is sought.

(4) For the purposes of subsection (3)(a), consent to the provision of information may be given –

(a) by the individual personally, if he or she has attained the age of 16 years; or

(b) by a representative of that individual.[[82]](#footnote-82)

The Police if they have a production order signed by a judge

Self explanatory. The rules around production orders are set out in the Search and Surveillance Act 2012.

The IRD under section 17 of the Tax Administration Act 1994

Section 17(1) provides that every person shall, when required by the Commissioner, furnish in writing any information and produce for inspection any documents which the Commissioner considers necessary or relevant for any purpose relating to the administration or enforcement of any of the Inland Revenue Acts or for any purpose relating to the administration or enforcement of any matter arising from or connected with any other function lawfully conferred on the Commissioner.

Where disclosure is not compulsory

If disclosure is not compulsory, the next question for the health provider is whether they can disclose. There are a wide range of discretionary grounds for disclosure, such as:

a) requests from Police officers, social workers, prison medical officers, probation officers, employees of the Ministry of Health, Ministry of Primary Industries, or Land Transport New Zealand or a DHB under section 22C of the Health Act

b) one of the grounds for disclosure in rule 11 of the HIPC applies (serious threat, avoiding prejudice to the maintenance of the law, or statistical/research purposes).

In many cases a disclosure to an official body will be permissible but not obligatory. In these cases it is up to the health provider to decide whether they want to disclose, and if so how much. This is the sort of question that should not be made on a purely ad hoc basis but should instead be made in accordance with information governance guidelines, for instance a DHB might have a policy that it will disclose information to Police only where it is necessary to prevent a serious threat to someone’s health or safety, or in response to a Court order (search warrant).

Potential future disclosure obligations

Section 66 Oranga Tamariki Act 1989 Children’s and Young People’s Well-being Act 1989

An amendment to this Act will come into force on a date appointed by Order in Council or on 1 July 2019 if it has not earlier been brought into force. The amendment will provide that every agency must on request by the Chief Executive (of a government department), a care and protection coordinator or constable, supply any information required to determine whether a child or young person is in need of care and protection under the Act or is required in regard to any proceedings under the Act (including a family group conference).[[83]](#footnote-83)

Some limited grounds for refusal apply (eg, legal or professional privilege).

Appendix 11: Information matching

Information matching can only be undertaken between the specified agencies listed in section 97 of the Privacy Act 1993. These agencies are:

* the Accident Compensation Corporation
* the Regulator, as defined by [Part 10](http://www.legislation.govt.nz/act/public/1993/0028/latest/link.aspx?id=DLM104120) of the Accident Compensation Act 2001
* the Electoral Commission established by [section 4B](http://www.legislation.govt.nz/act/public/1993/0028/latest/link.aspx?id=DLM2997501) of the Electoral Act 1993
* the company within the meaning of [section 2(1)](http://www.legislation.govt.nz/act/public/1993/0028/latest/link.aspx?id=DLM269435) of the Housing Restructuring and Tenancy Matters Act 1992
* the Board of the Government Superannuation Fund Authority
* the Board of Trustees of the National Provident Fund
* the Ministry of Health
* the Ministry of Justice
* the Department of Corrections
* the Ministry of Business, Innovation, and Employment
* the department for the time being responsible for the administration of the [Social Security Act 1964](http://www.legislation.govt.nz/act/public/1993/0028/latest/link.aspx?id=DLM359106)
* the Housing New Zealand Corporation established (as the Housing Corporation of New Zealand) by [section 3(1)](http://www.legislation.govt.nz/act/public/1993/0028/latest/link.aspx?id=DLM412001) of the Housing Corporation Act 1974
* the Inland Revenue Department
* the Ministry of Transport
* the New Zealand Transport Agency
* the Department of Internal Affairs
* the Registrar-General appointed under [section 79(1)](http://www.legislation.govt.nz/act/public/1993/0028/latest/link.aspx?id=DLM364757) of the Births, Deaths, Marriages, and Relationships Registration Act 1995
* the New Zealand Customs Service
* the Registrar of Motor Vehicle Traders
* the Regulator, as defined in the Accident Insurance Act 1998
* WorkSafe New Zealand
* any tertiary institution, secondary school, or private training establishment (as those terms are defined in the [Education Act 1989](http://www.legislation.govt.nz/act/public/1993/0028/latest/link.aspx?id=DLM175958)) to which [section 226A](http://www.legislation.govt.nz/act/public/1993/0028/latest/link.aspx?id=DLM185127) or section 238B of that Act applies, as from time to time notified to the Commissioner by the department for the time being responsible for the administration of the [Social Security Act 1964](http://www.legislation.govt.nz/act/public/1993/0028/latest/link.aspx?id=DLM359106)
* the Ministry of Education
* the New Zealand Teachers Council established under [Part 10A](http://www.legislation.govt.nz/act/public/1993/0028/latest/link.aspx?id=DLM181706) of the Education Act 1989
* the agency or agencies appointed under [section 100](http://www.legislation.govt.nz/act/public/1993/0028/latest/link.aspx?id=DLM5770797) of the Housing Restructuring and Tenancy Matters Act 1992.

Appendix 12: Approved information sharing agreement

Approved Information Sharing Agreements (AISAs) allow information sharing that would otherwise be unlawful between and within agencies to deliver public services.

Purpose

An AISA authorises the agencies that are parties to it to share personal information in order to provide a public service specified in the agreement.

AISAs change the rules around how agencies share personal information, while ensuring safeguards are in place to protect an individual’s privacy.

AISAs clarify and improve the rules around how the agencies share personal information Privacy Principles of codes of practice, while ensuring safeguards are in place to protect an individual’s privacy.

AISAs can modify or change most of the Privacy Act’s information [privacy principles](http://privacy.org.nz/the-privacy-act-and-codes/privacy-principles/) or [codes of practice](http://privacy.org.nz/the-privacy-act-and-codes/codes-of-practice/), for instance by allowing information to be used or disclosed for purposes other than the purpose for which it was obtained (Principles 10 and 11).

However, AISAs cannot modify or override information privacy principles 6 and 7, which allow a person to access and correct their personal information.

Parties

Government departments, non-government organisations and private sector agencies (including individuals) can enter into an AISA.

At least one of the parties must be a government department and the lead agency must be a government department.

An agency that represents the interests of members of a profession (such as doctors) or types of institutions (such as DHBs) can be party to an AISA. Such parties represent what are known as a ‘class of agencies’. The agreement must clearly define the members of the class.

Organisations or people outside New Zealand cannot be party to an AISA.

Content

An AISA must include certain features required by the Privacy Act, including the purpose of the agreement, privacy safeguards and what information will be shared and how. For details, see sections [96I](http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM5060448.html) and [96K](http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM5060451.html) of the Act.

Role of the Privacy Commissioner

The Privacy Commissioner has a strong oversight role for AISAs, both when they are being developed and once they are in effect.

Before approval

Agencies have to consult the Commissioner when drawing up information sharing agreements.

The Commissioner can report to lead agencies’ Ministers about privacy issues in draft agreements.

The Commissioner’s report must be taken into account before agreements are finalised.

After approval

The Privacy Commissioner may require the AISA’s lead agency to regularly report on the operation of the agreement.

The Commissioner can review an AISA and its operation and report to the lead agency’s Minister. After consulting the Minister the Commissioner may publish the report.

Other safeguards

Agencies must consult with representatives of those whose information would be shared.

Lead agencies’ ministers must be satisfied that AISAs do not unreasonably impinge on people’s privacy; that the benefits of agreements outweigh the costs; and that agreements contain adequate privacy safeguards.

AISAs must be accessible online, free of charge.

Other key points

AISAs are created when an information sharing agreement is approved by Order in Council on the recommendation of the Minister responsible for the AISA’s lead agency.

AISAs have the status of regulations. Therefore, they have a stronger legal authority than a memorandum of understanding to share information.

No person or organisation can be compelled to join an AISA.

AISAs authorise, but do not compel, parties to share information with each other.

Where Acts of Parliament prohibit information sharing, AISAs cannot override them.

Appendix 13: Secondary use of data

Secondary use of data – types and degrees of anonymisation

Types of data

#### Aggregate data

Data derived from records about more than one person, and expressed in summary form, such as statistical tables. Aggregate data usually presents little privacy risk.

#### Consumer level data

Consumer level data describes characteristics or events relating to individual consumers. Consumer level data can be classified as identifiable or non-identifiable. Consumer level data is identifiable if it includes data that indicates a consumer’s identity. Consumer data is non-identifiable if information that might identify a consumer has been removed. Even non-identifiable data may carry a risk of re-identification of a consumer if the data features uncommon characteristics (eg, a rare genetic disorder) or a deliberate attempt is made to link the data with other information about the target.

Methods for reducing risk of consumer identification

#### Obfuscation

Obfuscation is any process that decreases data precision to minimise re-identification risk. An example of obfuscation is the replacement of date of birth with year of birth.

#### De-identification

De-identification involves obfuscation or removal of direct identifiers such as names or email addresses and indirect identifiers such as date of birth or employer. De-identification is sufficient to prevent accidental identification of a consumer during data analysis. Consumers might still be identified through deliberate re-identification techniques involving linkage with other data sources.

#### Anonymisation

Anonymisation goes beyond de-identification by limiting the information content of consumer records to make linkages to other data sets difficult. Measures of anonymity include k‑anonymity and I-diversity.

#### k-anonymity

k-anonymity is a measure of anonymity in a data set. A data set provides k-anonymity if the data for each consumer is indistinguishable from at least k-1 other records. For example, in a data set with 5-anonymity every consumer shares the same characteristics with at least 4 others. k‑anonymity may be applied across all data points (strong k-anonymity) or only those considered likely to be found in other data sets that might be used for re-identification (weak k‑anonymity).

#### Pseudonymisation

Pseudonymisation assigns each consumer a unique identifier (pseudonym) which may be used for linking non-identifiable data sets without revealing consumer identity.

#### Encryption

Encryption is a secure reversible process that can be used to anonymise identifiable information in such a way that those with appropriate authorisation can re-identify consumers of interest following analysis of non-identifiable data (eg, identification to a general practitioner of an at-risk subset of the population requiring medical intervention).

#### Definition of identifiable data

Consumer data is considered identifiable if it includes any of the following:

* Direct identifiers
* NHI
* name
* street address
* phone number
* online identity (eg, email, twitter name)
* identification numbers (eg, community services card number, driver’s licence number).
* Indirect identifiers
* date of birth
* identification of relatives
* identification of employers
* clinical notes
* any other direct or indirect identifiers that carry significant risk of re-identification.

#### Definition of non-identifiable data

These guidelines defines two levels of non-identifiable data: de-identified data and anonymised data.

#### De-identified data

Consumer level data is considered de-identified if:

* fields listed under the definition of identifiable data are excluded, and
* fields that might be used for deliberate re-identification are included, such as:
* encrypted NHI
* year of birth or age in years at a given date
* event dates
* gender
* ethnicity (Level 2 as defined by Statistics New Zealand)
* mesh block or suburb
* deprivation index.

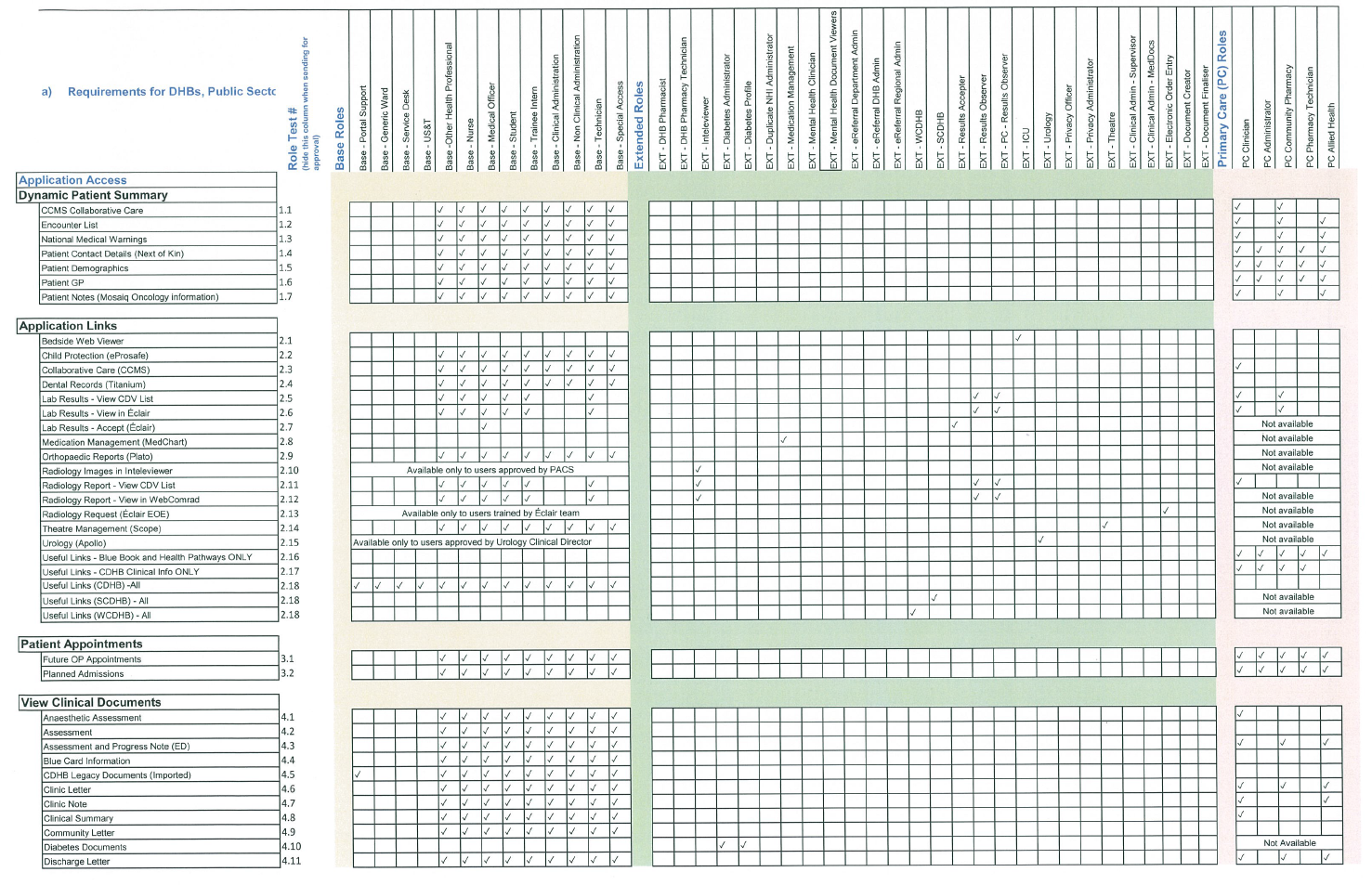
#### Anonymised data

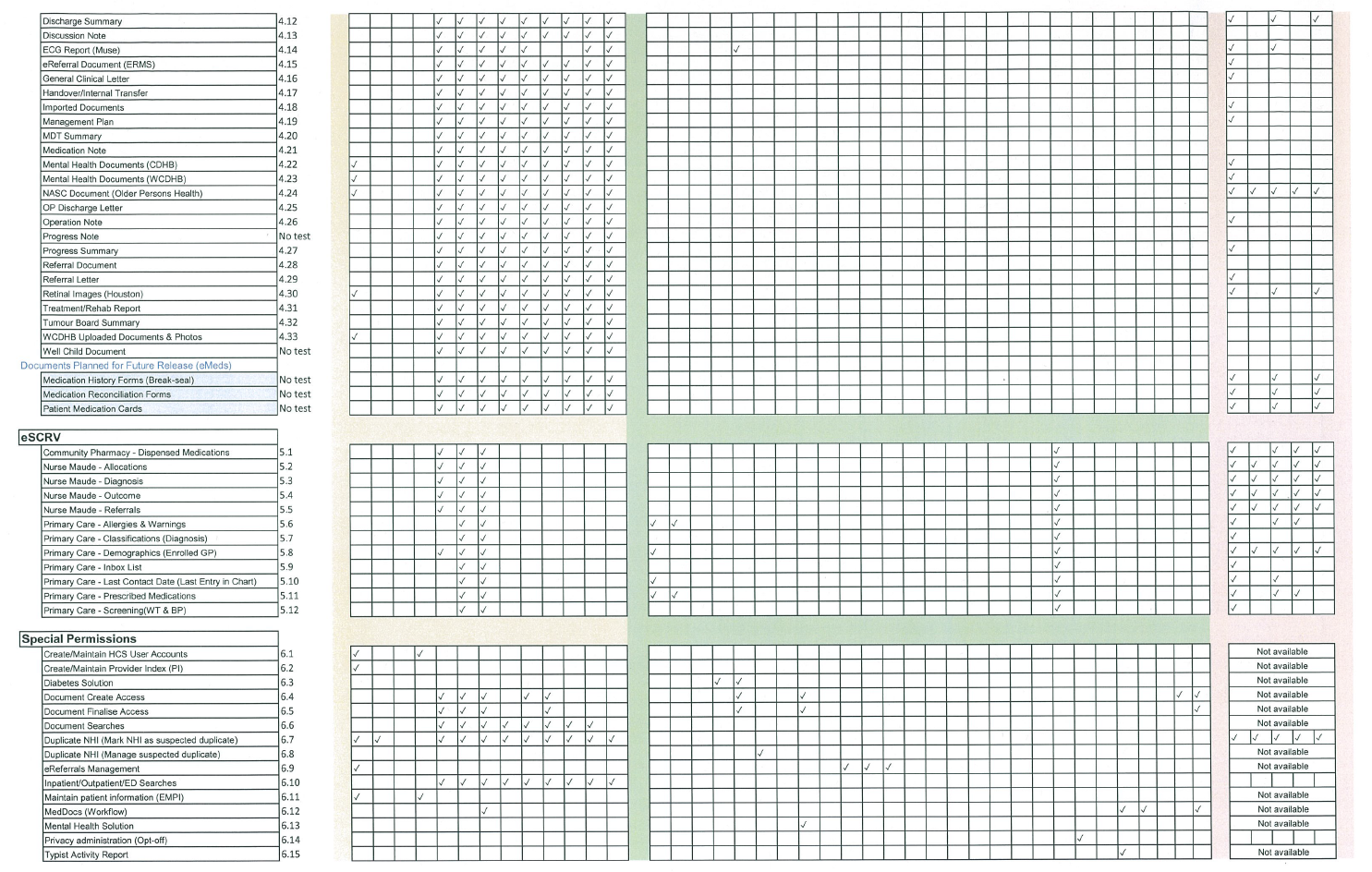
It is not possible to precisely define anonymised data as re-identification risk depends on characteristics of the specific data set and other data that it might be linked to. At a minimum, for consumer level data to be considered anonymised:

* fields listed under the definition of identifiable or de-identified data are excluded, and
* the data is obfuscated to minimise re-identification risk, including but not limited to the following measures:
* disclosure of the bare minimum data set for purpose
* use of 5–10-year bands rather than dates
* aggregation of ethnicity data (Level 1 as defined by Statistics New Zealand)
* blurring of geographic data (by area unit or city)
* exclusion of low-frequency characteristics useful for re-identification (eg, rare medical conditions)
* the resulting data set has k-anonymity ≥5.

Appendix 14: Example of role based access control matrix

Example of a role-based access control matrix for the South Island regional electronic health record system called HealthOne.







1. http://www.health.govt.nz/publication/hiso-100292015-health-information-security-framework [↑](#footnote-ref-1)
2. The original draft of this document was titled “The Health Information Governance Framework”. [↑](#footnote-ref-2)
3. Statement adapted from Health Information and Quality Authority *“Guidance on Information Governance for Health and Social Care Services in Ireland”* 2012, <http://hiqa.ie/healthcare/health-information/information-governance>, page 7. [↑](#footnote-ref-3)
4. Health Information Privacy Fact Sheet 1: https://privacy.org.nz/news-and-publications/guidance-resources/health-information-privacy-fact-sheet-1-overview/ [↑](#footnote-ref-4)
5. Section 22H of the Health Act 1956 allows anonymous health information to be used without restriction. [↑](#footnote-ref-5)
6. Medical Protection Society England Fact Sheets, Medical Records, April 2013, http://www.medicalprotection.org/uk/england-factsheets/medical-records [↑](#footnote-ref-6)
7. Cole’s Medical Practice in New Zealand, 2013 ed. Edited by Ian St George, MD, Medical Council of New Zealand, <https://www.mcnz.org.nz/assets/News-and-Publications/Coles/Coles-Medical-Practice-in-New-Zealand-2013.pdf> [↑](#footnote-ref-7)
8. Hunter I, Ede GH, Whiddett R. 2014. Increased electronic information sharing by sexual health services: Confidentiality and consent. *Health Informatics Journal* 20(1): 3–12. NHS Information Authority. 2002. *Share with Care! People’s Views on Consent and Confidentiality of Patient Information*. London. Riordan F, Papoutsi C, Reed JE, et al. 2015. Patient and public attitudes towards informed consent models and levels of awareness of Electronic Health Records in the UK*. International Journal of Medical Informatics* 84(4): 237–47.Whiddett R, Hunter I, Engelbrecht J, et al. 2006. Patients’ attitudes towards sharing their health information. *International Journal of Medical Informatics*. 75(7): 530–41. [↑](#footnote-ref-8)
9. Sankar P, Mora S, Merz JF, et al. 2003. Patient perspectives of medical confidentiality. *Journal of General Internal Medicine* 18(8): 659–69. Hunter I, Ede GH, Whiddett R. 2014. Increased electronic information sharing by sexual health services: confidentiality and consent. *Health Informatics Journal* 20(1): 3–12. [↑](#footnote-ref-9)
10. National Information Board and Department of Health. 2014. *Personalised Health and Care 2020: A guidance for action.* <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/384650/NIB_Report.pdf> [↑](#footnote-ref-10)
11. The New Zealand government defines ‘IN CONFIDENCE’ as information that if released “would be likely to prejudice the maintenance of law and order, impede the effective conduct of government in New Zealand or affect adversely the privacy of its citizens”. Department of Prime Minister and Cabinet, Cabinet Office Circular CO (08) 01 <http://www.dpmc.govt.nz/cabinet/circulars/co08/1>

    From a practitioner viewpoint, IN CONFIDENCE mirrors doctor patient confidentiality and means that a person’s health information won’t be disclosed unless consented to or authorised by that person (eg, through a privacy fact sheet), by another authorised person, under statutory authority or by a legal instrument (eg, an Approved Information Sharing Agreement), [↑](#footnote-ref-11)
12. Rules are paraphrased and the Health Information Privacy Code 1994 should be consulted for exact provisions: https://www.privacy.org.nz/assets/Files/Codes-of-Practice-materials/HIPC-1994-2008-revised-edition.pdf [↑](#footnote-ref-12)
13. Paragraph 5.14 on data quality has been adapted with revisions from the Health Information and Quality Authority *“Guidance on Information Governance for Health and Social Care Services in Ireland”* 2012, <http://hiqa.ie/healthcare/health-information/information-governance> [↑](#footnote-ref-13)
14. Health Record Standard NZS 8153:2002. This can be purchased through Standards New Zealand: <https://shop.standards.govt.nz/catalog/8153%3A2002(NZS)/view> [↑](#footnote-ref-14)
15. <http://legislation.govt.nz/regulation/public/1996/0343/latest/DLM225616.html> [↑](#footnote-ref-15)
16. https://privacy.org.nz/assets/Files/Codes-of-Practice-materials/HIPC-1994-incl.-amendments-revised-commentary-edit.pdf [↑](#footnote-ref-16)
17. See http://www.health.govt.nz/our-work/ehealth/digital-health-standards-and-governance/health-information-standards/approved-standards [↑](#footnote-ref-17)
18. Above footnote 7. [↑](#footnote-ref-18)
19. <https://www.mcnz.org.nz/assets/News-and-Publications/Statements/Maintenance-and-retention-of-records.pdf> [↑](#footnote-ref-19)
20. <http://shop.standards.co.nz/catalog/8153%3A2002(NZS)/view> [↑](#footnote-ref-20)
21. Section 23 Privacy Act 1993 and Regulation 7 of the Health Information Privacy Code 1994. [↑](#footnote-ref-21)
22. Regulation 7 (2) of the Health Information Privacy Code 1994 is partially relevant in that it requires every health agency to have a complaints policy in place that deals with alleged breaches of the Code. [↑](#footnote-ref-22)
23. https://privacy.org.nz/news-and-publications/guidance-resources/data-safety-toolkit/ [↑](#footnote-ref-23)
24. Privacy Impact Assessment Handbook, Office of the Privacy Commissioner 2007 p 5 <https://www.privacy.org.nz/assets/Uploads/Privacy-Impact-Assessment-Handbook-June2007.pdf> [↑](#footnote-ref-24)
25. Above, footnote 16, p11. [↑](#footnote-ref-25)
26. For details about eligibility see the Health and Disability Services Direction 2011. <http://www.health.govt.nz/system/files/documents/pages/eligibility-direction-2011.pdf> [↑](#footnote-ref-26)
27. It is noted that while most health providers should be able to advise of this in relation to electronic health records (by way of checking their audit log), this may not be possible in the case of paper records and therefore cannot be expected. [↑](#footnote-ref-27)
28. Section 27–29 of the Privacy Act 1993. [↑](#footnote-ref-28)
29. DeWalt DA, et al. 2010. *Health Literacy Universal Precautions Toolkit* (prepared by North Carolina Network Consortium, The Cecil G Sheps Center for Health Services Research, The University of North Carolina at Chapel Hill, under Contract No. HHSA290200710014). AHRQ Publication No. 10-0046-EF) Rockville, MD. Agency for Health Care Research and Quality. <http://www.ahrq.gov/professionals/quality-patient-safety/quality-resources/tools/literacy-toolkit/healthliteracytoolkit.pdf> [↑](#footnote-ref-29)
30. <http://www.ahrq.gov/professionals/quality-patient-safety/quality-resources/tools/literacy-toolkit/healthliteracytoolkit.pdf> [↑](#footnote-ref-30)
31. Rules 3 and 6 of the Health Information Privacy Code 1994 are particularly relevant here. [↑](#footnote-ref-31)
32. Rule 7, Privacy Act 1993. [↑](#footnote-ref-32)
33. Section 38 Privacy Act 1993. [↑](#footnote-ref-33)
34. Section 40 Privacy Act 1993. [↑](#footnote-ref-34)
35. Section 41 Privacy Act 1993. [↑](#footnote-ref-35)
36. Above footnote 32. [↑](#footnote-ref-36)
37. Above footnote 32. [↑](#footnote-ref-37)
38. Above footnote 32. [↑](#footnote-ref-38)
39. Also, see the Health Information Security Framework http://healthitboard.health.govt.nz/standards/approved-standards/hiso-100292015-health-information-security-framework. [↑](#footnote-ref-39)
40. Break glass indicates that access has been obtained in a non-routine way, generally because of emergency. Break glass incidents should be logged and audited. [↑](#footnote-ref-40)
41. New Zealand Health Strategy Future Direction, April 2016. Chapter 4 “One Team”. [↑](#footnote-ref-41)
42. Rule 5.2 Health Information Privacy Code 1994. [↑](#footnote-ref-42)
43. The thinking behind this section is based on a draft discussion document “Shared Electronic Health Records: Safe Sharing to Support Trust. A Discussion Document”. If you would like a copy of this document please contact [standards@moh.govt.nz](mailto:standards@moh.govt.nz) and request a copy. [↑](#footnote-ref-43)
44. Information taken from Office of the Privacy Commissioner website https://www.privacy.org.nz/further-resources/knowledge-base/view/374?t=59769\_77235 [↑](#footnote-ref-44)
45. See Appendix 1 for an overview of all relevant legislation relating to the Health and Disability Sector. [↑](#footnote-ref-45)
46. Rules 10 (and 11) Health Information Privacy Code 1994. For further information see Privacy Escalation Ladder – Appendix Four. [↑](#footnote-ref-46)
47. Section 22H Health Act 1956. [↑](#footnote-ref-47)
48. For further information on access control requirements see the Health Information Security Framework. <http://healthitboard.health.govt.nz/hiso-10029-health-information-security-framework> [↑](#footnote-ref-48)
49. Rules 10(1)(d) and 11(2)(d) HIPC. [↑](#footnote-ref-49)
50. Section 22F Health Act 1956 and Rule 4(b) Health Information Privacy Code 1994. [↑](#footnote-ref-50)
51. Rule 11(1)(e) HIPC. [↑](#footnote-ref-51)
52. Rule 11(2)(c) HIPC. [↑](#footnote-ref-52)
53. Where a health agency receives a complaint about a breach, they are required to acknowledge the complaint within five working days. Within 10 days after that they must decide whether they accept or reject the complaint, or determine if more time is needed to investigate the complaint. Section 7 HIPC 1994. [↑](#footnote-ref-53)
54. Refer HISO Standards – http://www.health.govt.nz/publication/hiso-100292015-health-information-security-framework [↑](#footnote-ref-54)
55. CAB-16-MIN-0316 [↑](#footnote-ref-55)
56. See Appendix 1 for an overview of all relevant legislation relating to the Health and Disability Sector. [↑](#footnote-ref-56)
57. Rules 10 (and 11) Health Information Privacy Code 1994. For further information see Privacy Escalation Ladder – Appendix Four. [↑](#footnote-ref-57)
58. Available at <http://privacy.org.nz/assets/Files/Codes-of-Practice-materials/HIPC-1994-incl.-amendments-revised-commentary.pdf> [↑](#footnote-ref-58)
59. Health (Retention of Health Information) Regulations 1996. [↑](#footnote-ref-59)
60. Section 9(2)(a), Official Information Act 1982. [↑](#footnote-ref-60)
61. Section 22C Health Act 1956. [↑](#footnote-ref-61)
62. Section 22F, Health Act 1956 (see also rule 11(4) of the HIPC). [↑](#footnote-ref-62)
63. Section 22H Health Act 1956. [↑](#footnote-ref-63)
64. NB: These two Acts, Oranga Tamariki Act 1989 and Child’s and Young Person’s Well-being Act 1989 are the same Act. In this document references to the Act will use the te Reo title Oranga Tamariki Act 1989. [↑](#footnote-ref-64)
65. Sections 15-16, Oranga Tamariki Act 1989. [↑](#footnote-ref-65)
66. Section 41, Children, Young Persons, and Their Families (Oranga Tamariki) Legislation Act 2017. [↑](#footnote-ref-66)
67. Version 2, July 2013. Published by the Institute of IT Professionals NZ. [↑](#footnote-ref-67)
68. NZS 8153:2002 NZS Health Records [↑](#footnote-ref-68)
69. Above footnote 68. [↑](#footnote-ref-69)
70. NZS 8153:2002 NZS Health Records, Information Privacy Code 1994 [↑](#footnote-ref-70)
71. For example, for funding validation, communicable disease notification, and quality improvement. [↑](#footnote-ref-71)
72. The opening paragraphs draw largely on the recent governance review undertaken in the UK. “Information: To share or not to share? The Information Governance Review”, UK March 2013. [↑](#footnote-ref-72)
73. Any information about the health of an identifiable consumer or patient. [↑](#footnote-ref-73)
74. See Rule 11(1)(e) of the Health Information Privacy Code 1994. [↑](#footnote-ref-74)
75. Section 22 H Health Act 1956 and Rule 11 of the Health Information Privacy Code 1993. [↑](#footnote-ref-75)
76. http://www.health.govt.nz/publication/hiso-100292015-health-information-security-framework [↑](#footnote-ref-76)
77. Extract taken from the Office of the Privacy Commissioner’s handbook: Privacy Impact Assessment Handbook. Section 4 “Why undertake Privacy Impact Assessment? https://privacy.org.nz/news-and-publications/guidance-resources/privacy-impact-assessment-handbook/ [↑](#footnote-ref-77)
78. Ministry for Primary Industries. Privacy Impact Assessment Guide, August 2014. [↑](#footnote-ref-78)
79. This is a summary of the purposes for obtaining information under section 11 of the Social Security Act 1964. To view the section go to <http://www.legislation.govt.nz/act/public/1964/0136/latest/DLM360781.html?search=ts_act%40bill%40regulation%40deemedreg_social+security+act_resel_25_a&p=1> [↑](#footnote-ref-79)
80. A copy of the Code of Conduct can be found at <https://www.msd.govt.nz/documents/about-msd-and-our-work/about-msd/legislation/code-of-conduct-section-11-ssa.pdf> [↑](#footnote-ref-80)
81. This is a summary of section 22F. To view the section in full go to <http://www.legislation.govt.nz/act/public/1956/0065/latest/DLM306662.html> [↑](#footnote-ref-81)
82. This is a summary of Section 17.of the Tax Administration Act 1994. To view the section go to http://www.legislation.govt.nz/act/public/1956/0065/latest/DLM306649.html [↑](#footnote-ref-82)
83. Section 41, Children, Young Persons, and Their Families (Oranga Tamariki) Legislation Act 2017. [↑](#footnote-ref-83)