Te Rēhita Whētuki o Aotearoa
New Zealand Trauma Registry

National Trauma Network

Privacy Framework for the

NZ Trauma Registry

Final

April 2021

Contents

Version control

Version	Comment / changes
2015	First version with the start of the NZ Trauma Registry on 1 July 2015
2020	Second version to incorporate changes associated with: New NZTR hosting and software Commission contract to provide functions to support the National Trauma Network Patient reported long term outcomes Utilisation of NZTR data for quality improvement, audit, and research with other datasets
2021	Incorporates changes associated with the Privacy Act 2020 and the Health Information Privacy Code 2020

Review of this Privacy Framework for the New Zealand Trauma Registry

Office of the Privacy Commissioner: The Office has been consulted in the development of this Framework and their feedback has been incorporated into this version of the document.

Accident Compensation Corporation Privacy Officer: The ACC Privacy Officer has been consulted in the development of this Framework and endorsed this version.

Accident Compensation Corporation Legal Counsel: The ACC Legal Counsel has been consulted in the development of this Framework and endorsed this version.

New Zealand Trauma Registry Data Governance Group: The NZTR Data Governance Group has endorsed this version of the Privacy Framework.

National Trauma Governance Group: Endorsed

Glossary

ACC	Accident Compensation Corporation
ATR	Australia (New Zealand) Trauma Registry
DHB	District Health Board
GDA	General Disposal Authority
HIPC	Health Information Privacy Code
IS	Information Systems
ISS	Injury Severity Score
NHI	National Health Index
NZTR	New Zealand Trauma Registry

Introduction

The NZ Trauma Registry Privacy Framework is updated to reflect the changes over the past five years as we progress to a more mature trauma system. It is a comprehensive framework which describes the measures taken to protect the privacy of patient information from the point of collection of information on trauma patients through to storage, access and use. It also responds to each of the 13 principles outlined in the Privacy Act 2020 and the corresponding Rules set out in the Health Information Privacy Code (HIPC) 2020.

There are two parts to this framework

- Part 1: General overview of the New Zealand Trauma Registry
- Part 2: Response to the 13 Rules of the HIPC 2020

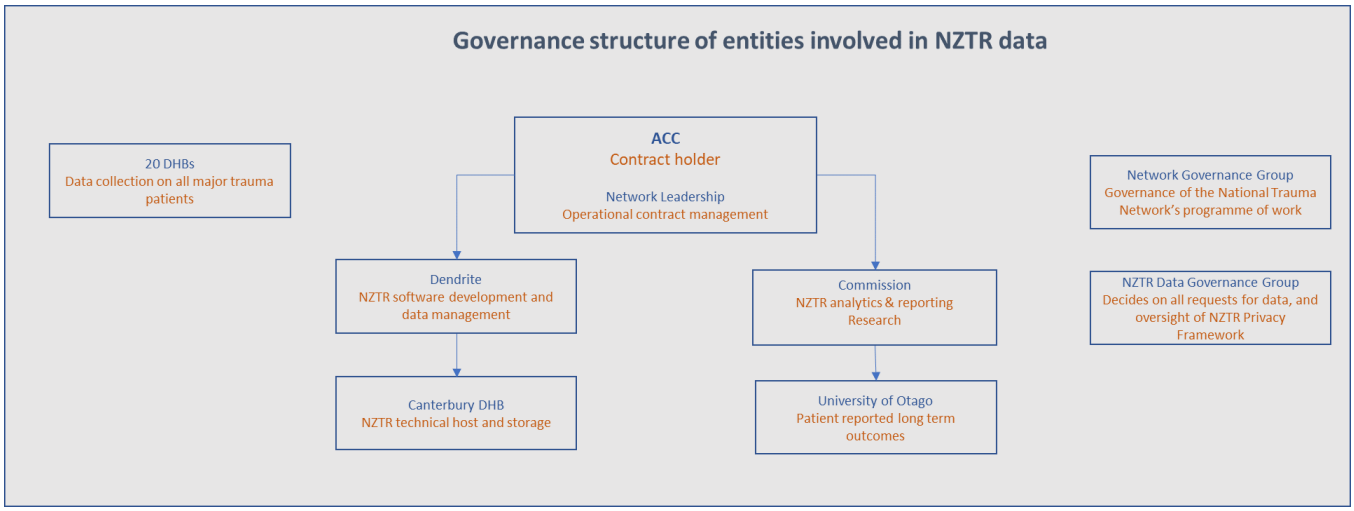
Part 1: General overview of the New Zealand Trauma Registry

The National Trauma Network (the Network) was established in 2012 with the mandate to establish a contemporary trauma system in New Zealand. It is funded by the Accident Compensation Corporation (ACC) and has three core objectives:

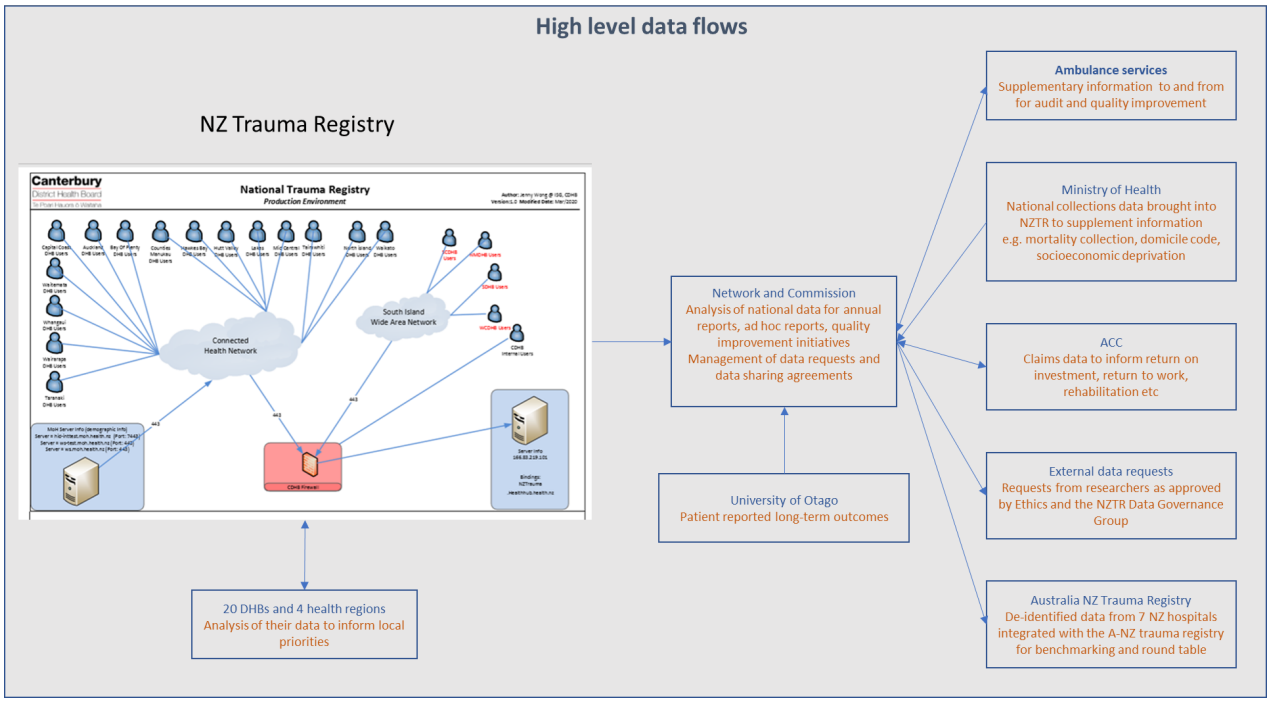
1. Save lives through reducing potentially avoidable deaths
2. Improve the quality of care for major trauma patients and improve recovery from injuries
3. Achieve efficiencies across the trauma system.

The Network manages the NZ Trauma Registry (NZTR) which is a national clinical quality registry of all people admitted to hospital with trauma who meet the inclusion criteria since 2015. The minimum dataset includes a sub-set of the patients' pre-hospital and hospital clinical record. The registry also includes patient reported outcomes at 6, 12 and 24 months post injury who are eligible and agree to be surveyed. The NZTR is the foundation for a contemporary, data-driven trauma system in New Zealand.

The following diagram shows the various organisations involved in data collection and management as they relate to this Privacy Framework.



The following diagram shows the high-level data flows.



The role of the NZTR Data Governance Group

The NZTR Data Governance Group has oversight of the NZTR Privacy Framework.

The NZTR Data Governance Group reviews all requests for data from the registry to ensure the request is an appropriate use of data, the correct ethics process has been established, and the relevant approvals received. The Data Governance Group is chaired by a clinician who is independent from the Network or any trauma registry. Membership comprises representation from the trauma regions, universities, Māori, the Health Quality and Safety Commission (Commission) and trauma nurses.

The role of the ACC

As primary sponsor of the NZTR, ACC has oversight of the functioning of the registry. While all personnel and agencies that input and use the NZTR data are bound by the Privacy Act 2020, ACC is the lead agency managing any risks and issues associated with the NZTR.

Legal framework for the NZTR

The framework for the collection, management and use of health information about individuals held within NZTR falls within the provisions of the HIPC 2020. The Privacy Act 2020 is also relevant as the overarching legislation governance the privacy of personal information in New Zealand. Other relevant legislation includes the Health Act 1956, the New Zealand Public Health and Disability Act 2000, the Public Records Act 2005, the DHB General Disposal Authority. The 13 rules articulated in the HIPC 2020 are used in this document as the framework of controls for the safe management of health information about identifiable individuals.

The primary ethical and privacy consideration of the NZTR is that of maintaining patient confidentiality across all steps in the gathering, storage and use of information. The remainder of this paper describes the measures taken to assure the privacy of personal information.

Reference documents

The following documents are referenced:

1. New Zealand Trauma Registry National Minimum Dataset Dictionary 2020
2. Protocol for Patient Reported Outcomes 2020
3. New Zealand Trauma Registry Data Use Policy 2020
4. New Zealand Trauma Registry Data Governance Group Terms of Reference 2020

Privacy Principles

The following are the privacy principles under which NZTR data is managed.

Collection

What information will be collected?

The New Zealand Trauma National Minimum Dataset details the data set being collected. Eligibility for entry to the Registry includes patients admitted to hospital after trauma and whose injuries are severe enough to meet the criteria that are set. Injuries are assessed using the Injury Severity Score (ISS) which is based on scoring the severity of each anatomical injury, and the higher the ISS, the greater the threat to life. This score is used in contemporary trauma systems worldwide and allows performance measures to be benchmarked like-with-like across different jurisdictions.

All patients who have an ISS score of 13 or more, or ISS under 13 and die after admission to hospital, are entered to the NZTR.

The data collected broadly includes:

Demographic data including the patient's name, date of birth, National Health Index, ethnicity, sex, and contact details

Incident details including the time and date of the injury, what the person was doing when they were injured, location, and description.

Pre-hospital information including vital signs such as heart rate, blood pressure, and Glasgow Coma Score. Information about how the patient was transported to hospital is also included.

Hospital information including the date and time of admission to hospitals the patient was taken to, vital signs, emergency procedures, diagnostic imaging, whether there were any serious missed injuries, and where the patient was discharged to.

In addition, the **Patient reported outcomes** including questions about their current health status, functional ability to perform daily activities, their recovery, and their living circumstances.

How will information be collected?

Information is collected in two different ways:

- Information about the patient, their treatment at the scene and in hospital, and the incident that caused the injury, is collected by trauma nurses and trauma data managers in each acute hospital in NZ. The

information is gathered from the patient's clinical record, which includes hospital and pre-hospital information.
- Information about patient reported outcomes is collected by telephoning trauma patients who have been entered into the Registry as a result of injury.

Why is this information collected?

Using the information collected will help us to understand the patterns of injury, the processes of care, and the outcomes for those injured. This will:

- Enable the Network to monitor and evaluate the effectiveness of the trauma system with the goal of reducing mortality, minimising disability for those that survive, and improving effectiveness of the trauma system as a whole
- Support audit and quality improvement activities to change the parts of the trauma system that could be improved
- Identify the issues that impact on recovery and chronic health impacts which result from injury.

How will individuals be informed that information is being collected?

The purpose for collecting personal information is clinical and covered by existing collection statements within each DHB. Each DHB has patient information pamphlets and posters that articulate what patients need to know about their health information (how it is collected, stored and used). Each DHB is required to have information accessible to all patients in line with the HIPC 2020.

A brochure about the trauma registry is available on the website and through the trauma services at each hospital. In addition, the brochure and a letter about the patient reported outcomes are posted to patients eligible for the patient reported outcomes interviews approximately five months after injury. Both documents provide information for individuals about how they can seek further information and how to opt-out if they wish.

Who handles this information?

People whose data is entered into the Registry own their information.

The handling of the NZ Trauma Registry dataset includes:

- DHBs for the data they submit to the NZTR
- Regions, where there is a regional agreement in place, for the region's data
- Dendrite and Canterbury DHB as the technical host and data managers of the NZTR
- National Trauma Network as the primary user of the NZTR for monitoring and evaluation of the trauma system from the point of injury through to rehabilitation
- The Commission which undertakes that analytics for the core registry data, the patient reported outcomes data, and supplementary data from other collections. The Commission leads the work to analyse the data for reporting purposes and quality improvement.
- University of Otago as the collectors of and hosts for the patient reported outcomes data until such time as it is transferred to the Commission and the National Trauma Network

The NZTR Data Governance Group is the entity accountable for NZTR data to ensure the use of data is ethical and appropriate. ACC has oversight of the NZTR.

Security

All data related to the NZTR is collected and stored in New Zealand.

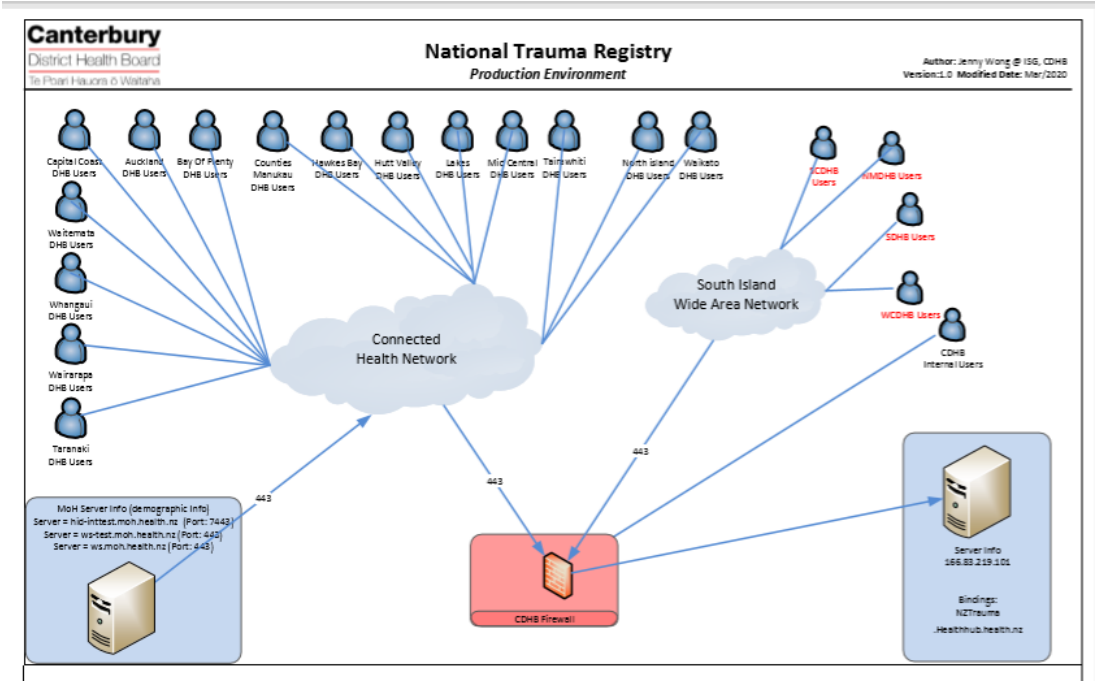
Collection at DHBs and input to the NZTR

The NZTR is operated across two data exchange networks:

- Connected Health Network for the 15 DHBs in the North Island. Connected Health is a standards-based, commercial model for the delivery of universal connectivity across the New Zealand health sector. It is overseen by the Ministry of Health. Connected Health aims to improve the reliability, safety, and security of transferring health information as only products or services certified against approved network connectivity standards will be allowed to connect to the network.
- South Island Wide Area Network.

The Registry is hosted by Canterbury DHB and falls within its IT Security Policy. Its physical location is in a secure data centre located at CCL 21 Durham Street, Christchurch, New Zealand. Dendrite manages the technical solution and data management of the NZTR and holds the contract with Canterbury DHB to host the data held in the registry. Dendrite is a registry software company based in the UK with a presence in New Zealand. The Registry data is held in NZ on servers located in Christchurch.

The following diagrams describes the Registry environment.



All authorised users are required to sign confidentiality statements and are DHB (or other organisation) employees with individual username and password allocated by a system administrator. All applications for access need to be approved by the National Programme manager of the Network. All users need to be assigned to a DHB and in a role that determines their permitted level of access to the NZTR. Controls to manage user identification include:

- New users are forced to change their password on first login
- Seven days before the password is due to expire, the user will be notified.
- If a user incorrectly enters their Username and/or Password three times, their account will be locked. After an account has been locked, (and upon request from the end-user) the System Administrator will issue a new password following which the user will be forced to change their password
- Only the NZTR System Administrator will have access rights to unlock/reset the password on any user account. Each time the NZTR System Administrator resets a password/unlocks an account, the user will be forced to change their password when they next enter the system.

- If the user does not try to log in during the seven-day grace period, the password will expire and a new password will need to be requested
- Dual User login is prohibited.

If a user is logged into the system and there is no activity on the page they are using, the system will time the user out of the system after 10 minutes and any data input on that page not submitted will be lost. The user will need to login to the system again to re-input data. The system idle timeout is maintained by the system administrator and can be configured, on a per user basis, up to a maximum of 9999 seconds.

Backup

Dendrite applications use InterSystems' Caché database for all data storage. Caché has a backup mechanism that can be configured to backup any or all of these CACHE.DAT files into a single unified backup file. These files are generated daily, on a weekly rolling basis.

Canterbury DHB Information Systems Group as the host server services is responsible for setting up server backup regimes.

Patient Reported Outcomes

Patient reported outcomes is a quality improvement project to understand the long-term outcomes of patients who have had major trauma and are entered into the NZTR. Eligible patients will be contacted at 6-, 12- and 24-months post injury by University of Otago interviewers. All information used to support and deliver the patient reported outcomes will be managed by the University of Otago and the Commission. The University of Otago and the Commission are responsible for the privacy of the data arising from the patient reported outcomes work.

Security arrangements at University of Otago include the following:

- All interviewers and team members are required to sign confidentiality agreements with the University of Otago and are supervised by the academic leads.
- Survey results are collected via REDCap which is accessible only to the University of Otago data collection team. Access to REDCap will be password protected. User-level security will be implemented, limiting which parts of the database the user can access or change. Personal identifying information stored on REDCap will be accessible to authorised (approved by the University of Otago) users only. The data will not be accessible to any individual who does not explicitly require access to collect or use the data or have ethics approval.
- File transfer from the University of Otago to the Commission is via a secure file transfer protocol. All files stored and transferred are encrypted.

Any data breaches will be notified to the Commission.

Commission and security of the NZTR data

The Commission has access to the NZTR under contract by ACC to deliver its role in the reporting and analysis of NZTR data, and to support quality improvement. The Commission's IT platform is hosted by CCL Revera (Spark) and is on an all-of-government infrastructure system as a service contract (IaaS). These contracts are overseen by the Department of Internal Affairs (DIA) and providers are required to meet security standards. Revera also provide network management and desktop support services. Database storage is on in-country servers located within their purpose-built data centres behind dedicated firewalls. Revera provide regular security patching for the Commission.

All staff have unique logins and database server access is separated and restricted to authorised staff. Once transferred, information is held in the Commission's secure data storage area, which can only be accessed specific Commission analytical teams or content specialists that work on programmes relevant to the project. All new (and existing) Commission staff are required to sign up to an IS information use policy, and in this context includes the Network leadership who fall within the Commission's IS policy. All laptops are protected using BitLocker.

Access

A relatively small number of users need to access the NZTR. This is likely to be one to two clinicians and/or administrators per DHB, analysts at the Commission, and the Network Leadership.

There are three levels of access:

- Hospital user access to enable view/edit/delete access in the user's hospital
- Regional access to enable view/edit/delete access for all DHBs within that region
- Super-user access to enable view/edit/delete access all hospital records.

Searching

Patients can be searched for by name, NHI, first name, last name.

Patient Access

All patients have the right to access information about them collected in the NZTR. There are several different ways to find out more information about the NZTR including:

- Asking the trauma service at the treating hospital
- Emailing: help@majortrauma.nz
- Free phone 0800 222 912

Patients will not be able to access the NZTR directly, however an extract of their information can be made available to them on request. Effort will be made to facilitate discussion between the patient and the hospital clinician to address any questions that may arise about their record.

Opting out

If a patient wishes to opt-out of the NZTR they can do so. This will be facilitated by the patient's health professional or contacting the NZTR directly via the email address or 0800 number.

If a patient wishes to stay in the Registry but opt-out of the patient reported outcomes, the Commission will inform the University of Otago and their information will be deleted from Otago's database.

Patient correction of information

If a patient wishes for their information to be corrected, depending on the nature of the request, the person making the request may be asked to put it in writing. The hospital trauma registry data manager, and/or the National Trauma Network (and its contracted partner the Commission) will facilitate the details of the request with the Registry Helpdesk.

If approval is not granted to correct the information, this will be worked through with the person who requested the change and their health care professional. A note will be made in the patient's entry on the NZTR setting the change request as provided by the patient and reason for decline.

Audit Log

All submissions of data into NZTR contains full details of who submitted that data. All patient movements and edits to the patient record are also logged and analysed as part of routine reporting. The NZTR also has the capability to audit who views a patient record. Audits will be undertaken on an as required basis and at minimum annually.

Inappropriate Access

Inappropriate access to information on the NZTR by any user is considered a serious breach of trust and would be a breach of the Confidentiality and Information Security Agreement that the user has signed. Inappropriate access includes any access to a patient record which is not necessary for the normal function of the NZTR. By way of example, inappropriate access may include accessing a patient entry without a valid purpose. The Chair of the NZTR Data Governance Group will take action, in accordance with due process and natural justice, which may involve informing the hospital employing the user of their concerns, removal of access privileges, referral to a relevant professional authority and notification to the Office of the Privacy Commissioner.

If necessary, the National Trauma Network Governance Group, which comprises senior representation from ACC, Ministry of Health, District Health Boards, NZ Transport Agency, and the Network, will take advice on managing inappropriate access or misuse of data.

Retention

DHB General Disposal Authority (GDA) guidelines require that health information be retained for a minimum of 10 years from the date of last contact.

The Privacy Act requires records be kept for no longer than is required for the purposes for which the information may be used.

The NZTR will keep records for a minimum of 10 years. After this time, it is expected that the information held in the Registry will continue to inform longitudinal analysis of trauma and measurement of system performance over time.

Disposal

The processes outlined in the Public Records Act 2005 Act will be adhered to by the NZTR.

Use of data

The role of the NZTR Data Governance Group is to ensure the use of NZTR data is ethical and appropriate.

The NZTR Data Use Policy describes how the data is used and the controls applied to ensure the use of data is ethical and appropriate.

Most individual DHBs will only have access to their own data unless an agreement exists for sharing of data between DHBs. Selected DHBs will have access to regional or national data as they provide tertiary or quaternary clinical care and are required to access records of patients transferred to their facility.

Aggregate data within the NZTR will be used for quality assurance and national research. This information will also form a basis (ethics dependent) for discrete pieces of research. Such requests for access to the data are made via a Data Access Proposal which must be approved by the NZTR Governance Group or their delegate, before data is released.

With the exception of the situation described in the paragraph below, requests for data to be provided from the NZTR to any external research or other external group will be serviced using patient level data with personal identifiers (i.e. NHI, names, date of birth) removed, or aggregate data.

In exceptional cases identifiable data (i.e. that containing NHI, name, date of birth) may be released under strict conditions. This may be required when, for example, to link data across other health databases for quality improvement and research. This is permitted within the exceptions of Rule 10(e)(i),(ii),(iii). The NZTR Data Governance Group takes into regard any conditions the Health and Disability Ethics Committee places on research proposals.

Data transfer

Once NZTR data has been authorised for approval it will be transmitted using the Revera product c-Stack Cache. This product has been assessed with Department of Internal Affairs cloud privacy risk assessment and uses 256 bit AES encryption at rest and in transit in line with Health Information Security Framework (HISO 10029:2015). All Cache data is hosted on Revera servers within New Zealand, in line with data sovereignty principles.

Disclosure

No third parties have access to the data within NZTR directly. Access to the NZTR is only through authorised access, and includes DHB staff with authority to access, and Dendrite and Canterbury DHB as hosts of the Registry,

Official Information Act requests may be made by members of the public from time to time in relation to the NZTR. Any data released under this Act will be patient anonymised (requests by the patient themselves will be dealt with under the Privacy Act/Health Information Privacy Code). The NZTR Data Governance Group will review all requests made under this Act and approve material to be released. The Ombudsman has final authority on release of information from the NZTR noting s9(2)(a) allows identifiable information to be withheld in most cases.

Unique Identifier

The NZTR uses the NHI number assigned to each patient. This is consistent with Schedule 2 of the HIPC 2020 and is necessary to identify patients as they move between hospitals. It will also maximise the value of the registry by allowing linkage to other health data.

Part 2: Response to Health Information Privacy Code

The following responses relate to the 13 principles outlined in the Health Information Privacy Code, 2020. The relevant extract is copied from the legislation for reference.

Rule 1: Purpose of collection of personal information

Rule 1
Purpose of collection of health information

(1) Health information must not be collected by a health agency unless—

(a) the information is collected for a lawful purpose connected with a function or activity of the health agency; and

(b) the collection of the information is necessary for that purpose.

(2) If the lawful purpose for which health information about an individual is collected does not require the collection of an individual's identifying information, the health agency may not require the individual's identifying information.

Only information necessary for monitoring and evaluation of the trauma system, trauma quality improvement activities, and other uses as approved by the NZTR Data Governance Group are collected and held in the NZTR.

Rule 2: Source of personal information

Rule 2
Source of health information

(1) If a health agency collects health information, the information must be collected from the individual concerned.

(2) It is not necessary for a health agency to comply with subrule (1) if the agency believes, on reasonable grounds,—

(a) that the individual concerned authorises collection of the information from someone else having been made aware of the matters set out in rule 3(1); or

(b) that the individual is unable to give their authority and the health agency having made the individual's representative aware of the matters set out in rule 3(1) collects the information from the representative or the representative authorises collection from someone else; or

(c) that compliance would—

(i) prejudice the interests of the individual concerned; or

(ii) prejudice the purposes of collection; or

(iii) prejudice the health or safety of any individual; or

(d) that compliance is not reasonably practicable in the circumstances of the particular case; or

(e) that the collection is for the purpose of assembling a family or genetic history of an individual and is collected directly from that individual; or

(f) that the information is publicly available information; or

(g) that the information—

(i) will not be used in a form in which the individual concerned is identified; or

(ii) will be used for statistical purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(iii) will be used for research purposes (for which approval by an ethics committee, if required, has been given) and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(h) that non-compliance is necessary—

(i) to avoid prejudice to the maintenance of the law by any public sector agency, including prejudice to the prevention, detection, investigation, prosecution, and punishment of offences; or

(ii) for the protection of public revenue; or

(iii) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or

(i) that the collection of the information is in accordance with an authorisation granted under section 30 of the Act.

The collection of the pre-hospital and hospital data is collected on exceptions 2(a), (d), or (g)(i),(ii), or (iii). The NZTR data collected in-hospital will generally not be collected directly from patients, and instead will be obtained from the hospital medical record of the patient. On occasion the patient may be asked for information that is not available in the notes, such as where the injury occurred was and whether seat belts or other protective devices were used.

The NZTR data collected through the patient reported outcomes work will be obtained directly by the individual, or their proxy if the injured person is not able to provide it directly.

Rule 3: Collection of information from subject

Rule 3
Collection of health information from individual

(1) If a health agency collects health information from the individual concerned, or from the individual's representative, the health agency must take any steps that are, in the circumstances, reasonable to ensure that the individual concerned (and the representative if collection is from the representative) is aware of—

- (a) the fact that the information is being collected; and
- (b) the purpose for which the information is being collected; and
- (c) the intended recipients of the information; and
- (d) the name and address of—
  - (i) the health agency that is collecting the information; and
  - (ii) the agency that will hold the information; and
- (e) whether or not the supply of the information is voluntary or mandatory and if mandatory the particular law under which it is required; and
- (f) the consequences (if any) for that individual if all or any part of the requested information is not provided; and
- (g) the rights of access to, and correction of, health information provided by rules 6 and 7.

(2) The steps referred to in subrule (1) must be taken before the information is collected or, if that is not practicable, as soon as practicable after it is collected.

(3) A health agency is not required to take the steps referred to in subrule (1) in relation to the collection of information from an individual, or the individual's representative, if that agency has taken those steps on a recent previous occasion in relation to the collection, from that individual or that representative, of the same information or information of the same kind, for the same or a related purpose.

(4) It is not necessary for a health agency to comply with subrule (1) if the agency believes on reasonable grounds,—

- (a) that compliance would—
  - (i) prejudice the interests of the individual concerned, or
  - (ii) prejudice the purposes of collection; or
- (b) that compliance is not reasonably practicable in the circumstances of the particular case; or
- (c) that non-compliance is necessary to avoid prejudice to the maintenance of the law by any public sector agency, including prejudice to the prevention, detection, investigation, prosecution, and punishment of offences.

The NZTR data collected in-hospital is a sub-set of their clinical record and covered by existing collection statements within each DHB. Each DHB has patient information pamphlets and posters which articulate what patients need to know about their health information.

Individuals who are entered into the Registry are informed about the Registry through the brochure which outlines what information is collected and how it is used. It also includes contact details if further information is requested. (Appendix A).

The patient reported outcomes project involves collecting information from people directly, and all the relevant requirements in Rule 3(1) or (3) are complied with as part of the consenting process prior to the interviews.

Rule 4: Method of Collection

Rule 4
Manner of collection of health information

(1) A health agency must collect health information only—

(a) by a lawful means; and

(b) by a means that, in the circumstances of the case (particularly in circumstances where personal information is being collected from children or young persons),—

(i) is fair; and

(ii) does not intrude to an unreasonable extent upon the personal affairs of the individual concerned.

All information entered into the Registry is collected by lawful and fair means.

In-hospital information is obtained from hospital medical records and on occasion and only if appropriate, directly from the patient.

Patient reported outcome information is collected direct from the patient through telephone surveys which are kept as short as possible so as not to be unreasonably intrusive.

Rule 5: Storage and security

Rule 5
Storage and security of health information

(1) A health agency that holds health information must ensure—

(a) that the information is protected, by such security safeguards as are reasonable in the circumstances to take, against—

(i) loss;

(ii) access, use, modification, or disclosure that is not authorised by the agency; and

(iii) other misuse;

(b) that, if it is necessary for the information to be given to a person in connection with the provision of a service to the health agency, including any storing, processing, or destruction of the information, everything reasonably within the power of the health agency is done to prevent unauthorised use or unauthorised disclosure of the information; and

(c) that, where a document containing health information is not to be kept, the document is disposed of in a manner that preserves the privacy of the individual.

(2) This rule applies to health information obtained before or after the commencement of this code.

This privacy framework details the specific steps taken to protect the information from the point of collection of data, the registry technical solution, access to the data, and use of the data.

Rule 6: Access to personal information

Rule 6
Access to personal health information

(1) An individual is entitled to receive from a health agency upon request—

(a) confirmation of whether the health agency holds any health information about them; and

(b) access to their health information.

(2) If an individual concerned is given access to health information, the individual must be advised that, under rule 7, the individual may request the correction of that information.

(3) The application of this rule is subject to—

(a) Part 4 of the Act (which sets out reasons for refusing access to information and procedural provisions relating to access to information); and

(b) clause 6 (which concerns charges).

(4) This rule applies to health information obtained before or after the commencement of this code.

The NZTR is obliged to receive and respond to information requests. Information about an individual can be supplied on request in a number of ways. Patients can ask for their information via the helpdesk phone line or email, or through their hospital clinician. Before any information is released, the NZTR will fulfil its responsibilities before giving access to personal information as set out in section 57 of the Privacy Act 2020.

57 Responsibilities of agency before giving access to personal information

If an agency receives a request to access personal information, the agency—

(a) may give access to the information only if the agency is satisfied of the identity of the requestor; and

(b) must not give access to the information if the agency has reasonable grounds to believe that the request is made under the threat of physical or mental harm; and

(c) must ensure, by the adoption of appropriate procedures, that any information intended for a requestor is received—

(i) only by that requestor; or

(ii) if the request is made by a requestor as the representative of an individual, only by the requestor or the individual; and

(d) must ensure that, if the request is made by a requestor as agent for an individual, the requestor has the written authority of the individual to obtain the information, or is otherwise properly authorised by the individual to obtain the information.

Rule 7: Correction

Rule 7
Correction of health information

(1) An individual whose health information is held by a health agency is entitled to request the agency to correct the information.

(2) A health agency that holds health information must, on request or on its own initiative, take such steps (if any) that are reasonable in the circumstances to ensure that, having regard to the purposes for which the information may lawfully be used, the information is accurate, up to date, complete, and not misleading.

(3) When requesting the correction of health information, or at any later time, an individual is entitled to—

(a) provide the agency with a statement of the correction sought to the information (a statement of correction); and

(b) request the agency to attach the statement of correction to the information if the agency does not make the correction sought.

(4) If a health agency that holds health information is not willing to correct the information as requested and has been provided with a statement of correction, the agency must take such steps (if any) that are reasonable in the circumstances to ensure that the statement of correction is attached to the information in a manner that ensure that it will always be read with the information.

(5) If a health agency corrects health information or attaches a statement of correction to health information, that agency must, so far as is reasonably practicable, inform every other person to whom the agency has disclosed the information.

(6) Subrules (1) to (4) are subject to the provisions of Part 4 of the Act (which sets out procedural provisions relating to the correction of personal information).

(7) This rule applies to health information obtained before or after the commencement of this code.

In-hospital information held about a patient is obtained from hospital medical records. Any request for a correction will be submitted to the health practitioners caring for the patient, and any correction they make will be updated to the NZTR. There may be a number of different ways a patient can request access their information and these are outlined in the patient brochure.

If the health practitioner declines to make any changes to a patient's record, and a patient disagrees with this assessment, a statement setting out the correction sought but not made can recorded in the comments section of a patient's record in the NZTR.

For the patient reported outcomes, if a patient wishes to correct a previously provided response, they can do this with the interviewer. No reason needs to be provided for the reason for the correction.

Rule 8: Accuracy

Rule 8
Accuracy, etc, of health information to be checked before use or disclosure

(1) A health agency that holds health information must not use or disclose that information without taking any steps that are, in the circumstances, reasonable to ensure that the information is accurate, up to date, complete, relevant and not misleading.

(2) This rule applies to health information obtained before or after the commencement of this code.

It is the health practitioners caring for a patient who are responsibility for the accuracy and currency of a patient's information.

If a person collecting data for the NZTR notes any inaccuracies in the hospital medical record they will inform the team caring for the patient, who will update the record.

For the long-term outcomes work, the accuracy of the information provided is based on the patient's responses.

Rule 9: Retention

Rule 9
Retention of health information

(1) A health agency that holds health information must not keep that information for longer than is required for the purposes for which the information may lawfully be used.

(2) Subrule (1) does not prohibit any agency from keeping any document that contains health information the retention of which is necessary or desirable for the purposes of providing health services or disability services to the individual concerned.

(3) This rule applies to health information obtained before or after the commencement of this code.

DHB General Disposal Authority (GDA) guidelines require that health information be retained for a minimum of 10 years from the date of last contact.

The Privacy Act 2020 requires records be kept for no longer than is required for the purposes for which the information may be used.

The NZTR will keep records for a minimum of 10 years. After this time it is expected that the information held in the Registry will continue to inform longitudinal analysis of trauma and measurement of system performance over time.

When the NZTR Data Governance Group deems that records are no longer required, records may be deleted as necessary and disposal will be undertaken in a manner that is in accordance with the Public Records Act 2005 General Disposal Authority for DHBs.

Rule 10: Limits on use of personal information

Rule 10
Limits on use of health information

(1) A health agency that holds health information that was obtained in connection with one purpose may not use the information for any other purpose unless the health agency believes on reasonable grounds,—

(a) that the use of the information for that other purpose is authorised by—

(i) the individual concerned; or

(ii) the individual's representative where the individual is unable to give their authority under this rule; or

(b) that the purpose for which the information is to be used is directly related to the purpose in connection with which the information was obtained; or

(c) that the source of the information is a publicly available publication and that, in the circumstances of the case, it would not be unfair or unreasonable to use the information; or

(d) that the use of the information for that other purpose is necessary to prevent or lessen a serious threat to—

(i) public health or public safety; or

(ii) the life or health of the individual concerned or another individual;

(e) that the information—

(i) is to be used in a form in which the individual concerned is not identified; or

(ii) is to be used for statistical purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(iii) is to be used for research purposes (for which approval by an ethics committee, if required, has been given) and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(f) that the use of the information for that other purpose is necessary—

(i) to avoid prejudice to the maintenance of the law by any public sector agency, including prejudice to the prevention, detection, investigation, prosecution, and punishment of offences; or

(ii) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation) or

(g) that the use of the information is in accordance with an authorisation granted under section 30 of the Act.

(2) A health agency that holds health information that was obtained from the testing or examination of a blood sample collected in connection with the Newborn Metabolic Screening Programme shall not use that information unless is believes, on reasonable grounds, that the use is in accordance with Schedule 3.

(3) This rule does not apply to health information obtained before 1 July 1993.

The NZTR holds information which is used for quality improvement and audit activities for the trauma system and are described in Rule 10(1)(e),(i),(ii), or (iii). Any information requested for research purposes requires approval from the NZTR Data Governance Group which ensures any application demonstrates that the appropriate level of ethical approval has occurred in accordance with the National Ethical Standards Health and Disability Research and Quality Improvement. It is a condition of all data releases that NZTR data cannot be released to a third party.

Rule 11: Limits on disclosure of personal information

Rule 11
Limits on disclosure of health information

(1) A health agency that holds health information must not disclose the information unless the agency believes, on reasonable grounds,—

(a) that the disclosure is to—

(i) the individual concerned; or

(ii) the individual's representative where the individual is dead or is unable to exercise their rights under these rules; or

(b) that the disclosure is authorised by—

(i) the individual concerned; or

(ii) the individual's representative where the individual is dead or is unable to give their authority under this rule; or

(c) that the disclosure of the information is one of the purposes in connection with which the information was obtained; or

(d) that the source of the information is a publicly available publication and that, in the circumstances of the case, it would not be unfair or unreasonable to disclose the information; or

(e) that the information is information in general terms concerning the presence, location, and condition and progress of the patient in a hospital, on the day on which the information is disclosed, and the disclosure is not contrary to the express request of the individual or their representative; or

(f) that the information to be disclosed concerns only the fact of death and the disclosure is by a health practitioner or by a person authorised by a health agency, to a person nominated by the individual concerned, or the individual's representative, partner, spouse, principal caregiver, next of kin, whānau, close relative, or other person whom it is reasonable in the circumstances to inform; or

(g) that the information to be disclosed concerns only the fact that an individual is to be, or has been, released from compulsory status under the Mental Health (Compulsory Assessment and Treatment) Act 1992 and the disclosure is to the individual's principal caregiver.

(2) Compliance with subrule (1)(b) is not necessary if the health agency believes on reasonable grounds, that it is either not desirable or not practicable to obtain authorisation from the individual concerned and—

(a) that the disclosure of the information is directly related to one of the purposes in connection with which the information was obtained; or

(b) that the information is disclosed by a health practitioner to a person nominated by the individual concerned or to the principal caregiver or a near relative of the individual concerned in accordance with recognised professional practice and the disclosure is not contrary to the express request of the individual or their representative; or

(c) that the information—

(i) is to be used in a form in which the individual concerned is not identified; or

(ii) is to be used for statistical purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(iii) is to be used for research purposes (for which approval by an ethics committee, if required, has been given) and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(d) that the disclosure of the information is necessary to prevent or lessen a serious threat to—

(i) public health or public safety; or

(ii) the life or health of the individual concerned or another individual; or

(e) the disclosure of the information is necessary to enable an intelligence and security agency to perform any of its functions; or

(f) that the disclosure of the information is essential to facilitate the sale or other disposition of a business as a going concern; or

(g) that the information to be disclosed briefly describes only the nature of injuries of an individual sustained in an accident and that the individual's identity and the disclosure is—

(i) by a person authorised by the person in charge of a hospital; and

(ii) to a person authorised by the person in charge of a news entity;

and for the purpose of publication or broadcast in connection with the news activities of that news entity and the disclosure is not contrary to the express request of the individual concerned or their representative; or

(h) that the disclosure of the information—

(i) is required for the purpose of identifying whether an individual is suitable to be involved in health education and so that individuals so identified may be able to be contacted to seek their authority in accordance with subrule (1)(b); and

(ii) is by a person authorised by the health agency to a person authorised by a health training institution; or

(i) that the disclosure of the information—

(i) is required for the purpose of a professionally recognised accreditation of a health or disability service; or

(ii) is required for a professionally recognised external quality assurance programme; or

(iii) is required for risk management assessment and the disclosure is solely to a person engaged by the agency for the purpose of assessing the agency's risk;

and the information will not be published in a form which could reasonably be expected to identify any individual nor disclosed by the accreditation quality assurance or risk management organisation to third parties except as required by law; or

(j) that non-compliance is necessary—

(i) to avoid prejudice to the maintenance of the law by any public sector agency, including prejudice to the prevention, detection, investigation, prosecution and punishment of offences; or

(ii) for the conduct of proceedings before any court or tribunal (being proceedings that have commenced or are reasonably in contemplation); or

(k) that the individual concerned is or is likely to become dependent upon a controlled drug, prescription medicine, or restricted medicine and the disclosure is by a health practitioner to a Medical Officer of Health for the purposes of section 20 of the Misuse of Drugs Act 1975 or section 49A of the Medicines Act 1981; or

(l) that the disclosure of the information is in accordance with an authorisation granted under section 30 of the Act

(3) A health agency that holds health information that was obtained from the testing or examination of a blood sample collected in connection with the Newborn Metabolic Screening Programme shall not disclose that information unless it believes, on reasonable grounds, that the disclosure is in accordance with Schedule 3.

(4) Disclosure under subrule (2) is permitted only to the extent necessary for the particular purpose.

(5) Where under section 22F(1) of the Health Act 1956, the individual concerned or a representative of that individual requests the disclosure of health information to that individual or representative, a health agency—

(a) must treat any request by that individual as if it were a health information privacy request made under rule 6; and

(b) may refuse to disclose information to the representative if—

(i) the disclosure of the information would be contrary to the individual's interests; or

(ii) the agency has reasonable grounds for believing that the individual does not or would not wish the information to be disclosed; or

(iii) there would be good grounds for withholding the information under Part 4 of the Act if the request had been made by the individual concerned.

(6) This rule applies to health information about living or deceased persons obtained before or after the commencement of this code.

(7) Despite subrule (6), a health agency is exempted from compliance with this rule in respect of health information about an identifiable deceased person who has been dead for not less than 20 years.

(8) This rule is subject to rule 12.

Disclosure of health information will be made in the event the individual or their representative requests the information, and the information is released to them (Rule 11(1)(a) or (b)). Disclosure of health information may also be made under exceptions 11(2)(c)(i),(ii), or (iii) for the purposes of statistical or research purposes.

The NZTR Data Use Policy describes the use of data held in the NZTR and has been endorsed by the NZTR Data Governance Group The NZTR Data Governance Group reviews all requests for data to ensure compliance with this Privacy Framework and that the data request has received appropriate ethical approval, and is appropriate for use.

It is noted that identifiable patient data is provided only by exception. The reason for the exception must be clearly articulated and approval is granted only if absolutely necessary and with appropriate ethical approval. This may be required when, for example, linkage between different databases is required for research. This is allowed under the exceptions 11(2)(c)(ii), or (iii).

Rule 12: Disclosure of personal information outside New Zealand

Rule 12
Disclosure of health information outside New Zealand

(1) A health agency (A) may disclose health information to a foreign person or entity (B) in reliance on Rule 11(1)(b) or (c) or 11(2)(a), (c), (d), (f), (i) (j) or (l) only if—

(a) the individual concerned or, where the individual is dead or unable to exercise their rights under these rules, that individual's representative authorises the disclosure to B after being expressly informed by A that B may not be required to protect the information in a way that, overall, provides comparable safeguards to those in the Act, as modified by this code; or

(b) B is carrying on business in New Zealand and, in relation to the information, A believes on reasonable grounds that B is subject to the Act, as modified by this code; or

(c) A believes on reasonable grounds that B is subject to privacy laws that, overall, provide comparable safeguards to those in the Act, as modified by this code; or

(d) A believes on reasonable grounds that B is a participant in a prescribed binding scheme; or

(e) A believes on reasonable grounds that B is subject to privacy laws of a prescribed country; or

(f) A otherwise believes on reasonable grounds that B is required to protect the information in a way that, overall, provides comparable safeguards to those in the Act, as modified by this code (for example, pursuant to an agreement entered into between A and B); or

(g) that the disclosure of the information is in accordance with an authorisation granted under section 30 of the Act.

(2) However, subrule (1) does not apply if the health information is to be disclosed to B in reliance on Rule 11(2)(d) or (j) and it is not reasonably practicable in the circumstances for A to comply with the requirements of subrule (1).

(3) In this rule,—

prescribed binding scheme means a binding scheme specified in regulations made under section 213 of the Act

prescribed country means a country specified in regulations made under section 214 of the Act that are made without any qualification or limitation relating to a class of person that includes B, or to a type of information that includes health information.

NZTR data is sent overseas under exception 12(1)(f) whereby the NZTR Data Governance Group believes on reasonable grounds that the overseas entity receiving the data provides comparable safeguards to those in the New Zealand Privacy Act 2020. By way of example, this may include:

- Data sent to the Australian Trauma Registry (ATR) in a de-identified form for bi-national benchmarking to evaluate our performance against a much larger dataset. The ATR data is held within the IT infrastructure of Alfred Health in the State of Victoria, Australia. The Australian Privacy Act 1988 applies to the use of the New Zealand data held by the ATR, and is specified within the contract with Alfred Health. The contract specifies there is no third-party access to NZTR data
- NZTR data sent to entities in Australia which hold other New Zealand data sets
- International research which is important to understand the epidemiology, process of care and outcomes of injury in NZ comparable to other jurisdictions.

The NZ Trauma Registry Data Governance Group assesses all applications for research to ensure they ethical and culturally and scientifically appropriate. The NZ Data Governance Group will assess all requests to send NZTR data outside of New Zealand with particular consideration to Rule 11(2)(c)(i),(ii), or (iii) for the purposes of statistical or research purposes, and Rule 12((1)((f) on the understanding that the overseas entity receiving the data provides comparable safeguards to New Zealand. At the time of writing, it is believed on reasonable grounds that Australia and countries which fall within the European Union's General Data Protection Regulations have comparable safeguards to New Zealand's privacy laws.

Privacy Principle 13: Unique Identifiers

Rule 13
Unique Identifiers

(1) A health agency (A) may assign a unique identifier to an individual for use in its operations only if that identifier is necessary to enable A to carry out 1 or more of its functions efficiently.

(2) A may not assign to an individual a unique identifier that, to A's knowledge, is the same unique identifier as has been assigned to that individual by another agency (B), unless—

(a) A and B are associated persons within the meaning of subpart YB of the Income Tax Act 2007; or

(b) the unique identifier is to be used by A for statistical or research purposes and no other purpose; or

(c) it is permitted by subrule (3) or (4).

(3) The following agencies may assign the same National Health Index number to an individual—

(a) any agency authorised expressly by an enactment; or

(b) any agency or class of agencies listed in Schedule 2.

(4) Notwithstanding subrule (2) any health agency may assign to a health practitioner as a unique identifier—

(a) the registration number assigned to that individual by the relevant health professional body; or

(b) the Common Provider Number assigned to that individual by the Ministry of Health.

(5) To avoid doubt, A does not assign a unique identifier to an individual under subrule (1) by simply recording a unique identifier assigned to the individual by B for the sole purpose of communicating with B about the individual.

(6) A must take any steps that are, in the circumstances, reasonable to ensure that—

(a) a unique identifier is assigned only to individuals whose identity is clearly established; and

(b) the risk of misuse of a unique identifier by any person is minimised (for example, by showing truncated account numbers on receipts or in correspondence).

(7) A health agency may not require an individual to disclose any unique identifier assigned to that individual unless the disclosure is for one of the purposes in connection with which that unique identifier was assigned or for a purpose that is directly related to one of those purposes.

(8) Subrules 13(1) to (6)(a) do not apply to unique identifiers assigned before 30 July 1994.

(9) However, subrule 13(2) applies to the assignment of a unique identifier on or after 30 July 1994 even if the unique identifier is the same as that assigned by another agency before that date.

The NZTR uses the NHI to identify patients, in a manner consistent with other registries and quality assurance groups. Clause (3)(b) applies to the use of the NHI in the use of the NZTR. The use of the NHI number is consistent with Schedule 2 of the HIPC.

Appendix A: Brochure about the NZTR

Please follow this link for the brochure

https://www.majortrauma.nz/assets/Publication-Resources/NZ-MTR/Registry-Brochure-v12-FINAL.pdf