Te Rēhita Whētuki o Aotearoa
New Zealand Trauma Registry

National Trauma Network

Privacy Framework for the

NZ Trauma Registry

Final draft

21 September 2020

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

Review of this Privacy Framework for the New Zealand Trauma Registry

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

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

New Zealand Data Governance Group: The NZTR Data Governance Group has endorsed this Framework.

National Trauma Governance Group: Endorsement Pending

Overview

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 12 principles outlined in the Privacy Act, 1993.

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:

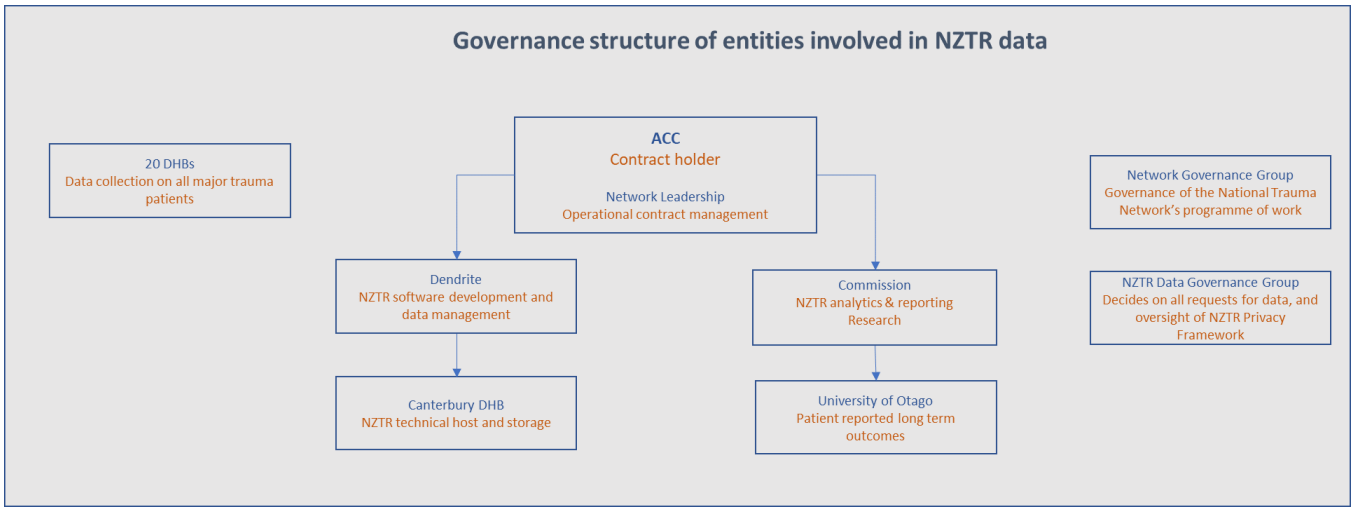
1. Save lives through reducing potentially avoidable deaths
2. Improve the quality of care for major trauma patients and improve recovery from injuries
3. Achieve efficiencies across the trauma system.

The Network manages the NZ Trauma Registry (NZTR) which is the foundation for a contemporary, data-driven trauma system in New Zealand. It 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 the patient reported outcomes at 6, 12 and 24 months post injury.

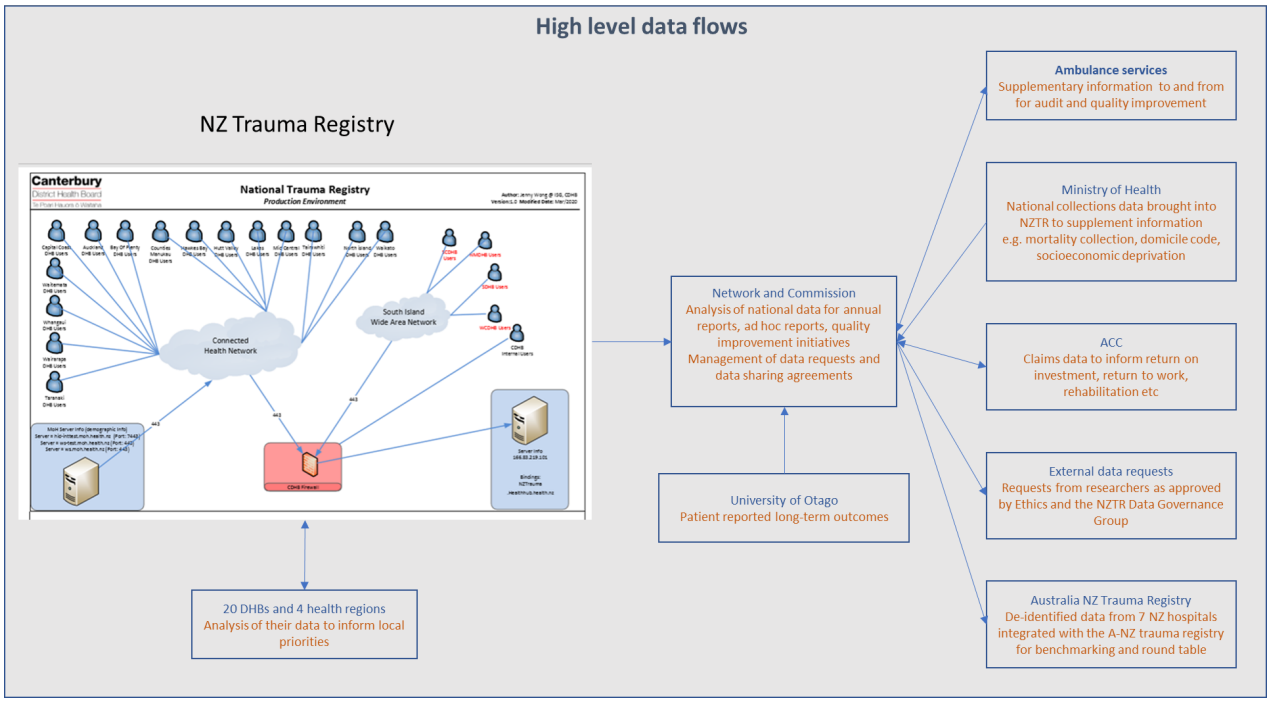
The key changes which are reflected in this updated Privacy Framework include:

- Changes to the hosting and software arrangements for a new national trauma registry (the 'NZTR').
- The role of the Health Quality and Safety Commission (the 'Commission ') which has been contracted by ACC on behalf of the Network to deliver several functions, including analytics, quality improvement, research, and the collection of patient-reported long-term outcomes.
- Patient reported long term outcome measures from 1 July 2020.
- Utilisation of NZTR data, in combination with other datasets, to contribute to our understanding of the patterns of injury and gaps in services.

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 is the 'owner' 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 Commission and trauma nurses.

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 Health Act 1956, the New Zealand Public Health and Disability Act 2000, the Privacy Act 1993, the Public Records Act 2005, Public Records Act 2005, DHB General Disposal Authority and the Health Information Privacy Code 1994 (HIPC). The HIPC, in particular, provides a broad framework of controls for the safe management of 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 and storage of the long-term outcome 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. Generally, patients are not directly asked to provide information.
- Information about long-term patient experience 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 Health Information Privacy Code 1994.

A brochure about the trauma registry is available on the website and through the trauma services at each hospital. The brochure and a letter about the patient reported outcomes will also be posted to eligible patients approximately five months after injury. Copies of these are found in Appendix A and B. Both documents provide information for individuals about how they can seek further information and how to opt-out if they wish.

Who owns this information?

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

The custodianship 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
- 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 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.

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

Security

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

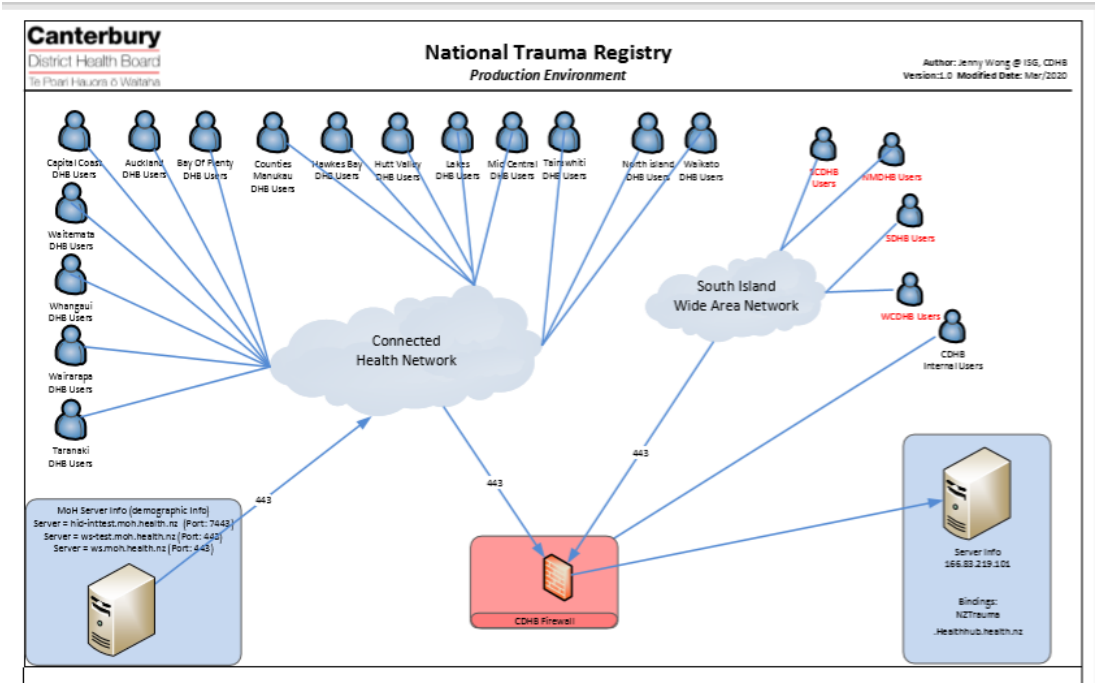
Collection at DHBs and input to the NZTR

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 following diagrams describes the Registry environment.



All DHB authorised users are required to sign confidentiality statements and are DHB 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

All information used to support and deliver the patient reported outcomes will be managed by the University of Otago and the Commission.

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.

Commission and security of the NZTR data

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 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.

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. 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 as required.

Inappropriate Access

Inappropriate access to information on the NZTR by any user is considered a serious breach of trust. 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.

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.

In general, data that could identify patients. will not be provided from the NZTR to any external research or other external group. Data requests will be serviced using unidentifiable patient level, or aggregate data (also non-identifiable).

In exceptional cases, and with ethics and other appropriate approvals, identifiable data by live NHI may be released under strict conditions. This may be required when, for example, cross match between different databases is required for research. 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 as an identifier. This is consistent with current sector standards and is necessary for the programme to identify patients as they move between hospitals. It will also maximise the value of the registry by allowing linkage to other data sources such as death registry, ACC, rehabilitation and hospital record collections.

Response to Privacy Act Principles

The following responses relate to the 12 principles outlined in the Privacy Act, 1993. It is noted this Act has been updated and the new Privacy Act 2020 will come into force on 1 December 2020. A review of the new Act indicates there are no material impacts between the two Acts as they relate to the New Zealand Trauma Registry.

Privacy Principle 1: Purpose of Collection

An agency must not collect information unless the information is necessary for one or more of its functions or activities.

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 will be extracted from a patient's record.

Privacy Principle 2: Source of information

When collecting information, it shall be done so straight from the subject unless there are reasonable grounds to believe that:

- *(a) the information is publicly available; or*
- *(b) the subject authorises collection from someone else; or*
- *(c) it wouldn't prejudice the subject if it wasn't collected from them; or*
- *(d) to collect from them would prejudice the purposes of collection; or*
- *(e) that compliance would prejudice the purposes of the collection; or*
- *(f) it is not practicable; or*
- *(g) the subject would not be identified; or*
- *(h) the information is in accordance with an authority granted under section 54.*

The collection of the pre-hospital and hospital data is collected on exceptions c and f. 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 accident 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.

Privacy Principle 3: Notice to Subject

Before the agency collects information from an individual (or, if that is not practicable, as soon as practicable thereafter) the agency must take reasonable steps to inform the individual of:

- *(a) the fact the information is being collected; and*
- *(b) the purposes for which the information is collected; and*
- *(c) to whom (or the types of organisations to which) the organisation usually discloses information of that kind; and*
- *(d) the identity of the organisation and how to contact it; and*
- *(e) any law that requires the particular information to be collected; and*
  the main consequences (if any) for the individual if all or part of the information is not provided

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).

Privacy Principle 4: Method of Collection

An agency must collect information only by lawful and fair means and not in an unreasonably intrusive way.

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 to not be unreasonably intrusive.

Privacy Principle 5: Information Security

An agency must take reasonable steps to protect the information it holds from misuse and loss and from unauthorised access, modification or disclosure.

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.

Privacy Principle 6: Access

If an agency holds information about an individual, it must provide the individual with access to the information on request by them, unless an exception applies.

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.

Privacy Principle 7: Correction

If an agency holds information about an individual and the individual is able to establish that the information is not accurate, complete and up to date, the agency must take reasonable steps to correct the information so that it is accurate, complete and up to date.

An agency must provide reasons for a refusal to correct information.

If the individual and the agency disagree about whether the information is accurate, the individual may request that the agency attach to the information a statement setting out the correction sought, but not made.

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.

If the health practitioners decline 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.

Privacy Principle 8: Accuracy

An agency must take reasonable steps to make sure that the information it collects, uses or discloses is accurate, complete and up to date.

It is the health practitioners caring for the patient that takes 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 patients responses.

Privacy Principle 9: Retention

Retention - An agency must not keep information for longer than is required for the purposes for which the information may be used.

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.

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.

Privacy Principle 10: Limits on use of personal information

An agency that holds personal information that was obtained in connection with one purpose shall not use the information for any other purpose unless the agency believes, on reasonable grounds,-

(a) That the source of the information is a publicly available publication; or

(b) That the use of the information for that other purpose is authorised by the individual concerned;

or

(c) That non-compliance is necessary -

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

(ii) For the enforcement of a law imposing a pecuniary penalty; or

(iii) For the protection of the public revenue; or

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

or

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

(i) Public health or public safety; or

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

or

(e) That the purpose for which the information is used is directly related to the purpose in connection with which the information was obtained;

or

(f) That the information-

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

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

or

(g) That the use of the information is in accordance with an authority granted under section 54

of this Act.

Information will be used for quality improvement and audit activities for the trauma system. Any information requested for research purposes requires demonstration that the appropriate level of ethical approval has occurred in accordance with the National Ethical Standards Health and Disability Research and Quality Improvement. The NZTR Data Governance Group reviews all requests for NZTR data to ensure they are ethical and appropriate, and aligned to the objective to improve outcomes for people who have been seriously injured. It is a condition of all data releases that NZTR data cannot be released to a third party.

Privacy Principle 11: Disclosure

An agency must not disclose information about an individual unless –

(a) it is consented to or authorised by the individual (or representative);

(b) the disclosure is one of the purposes of collection;

(c) the source is a publically available publication;

(d) the information discloses very general information; the fact of death; or if a person has been released from compulsory status under the Mental Health Act;

(e) disclosure is done so by a health practitioner in accordance with a code of professional practice and isn't expressly contrary to the individual's requests;

(f) use of the information is necessary to prevent or lessen serious threat to public health or safety or life or health of any individual;

(g) the information is to be used for statistical or research purposes and the individual will not be identified;

(h) the disclosure is authorised by a person in charge of the hospital and includes a brief description of the nature of injuries.

The NZTR Data Use Policy, which describes the use of data held in the NZTR, has been agreed by the NZTR Data Governance Group.

Aggregate data within the NZTR will be used for quality improvement and national research. This information will also form a basis for audit. For example, to understand the burden of deaths due to haemorrhage.

Any use of data which does not fall within audit or quality improvement must be approved by the NZTR Data Governance Group before data is released.

Identifiable patient data is provided only by exception to any external research or other external group which could identify patients. The reason for the exception must be clearly articulated and approval is granted only if absolutely necessary.

In exceptional cases, and with ethics and other appropriate approval, identifiable data may be released under strict conditions. This may be required when, for example, cross match between different databases is required for research. Once the match is made, the unique identifier is applied and the identifiable information is deleted or held under tight security accessible only by authorisation.

Privacy Principle 12: Unique Identifiers

A health agency must not assign a unique identifier to an individual unless the assignment of that identifier is necessary to enable the health agency to carry out any 1 or more of its functions efficiently.

A health agency must not assign to an individual a unique identifier that, to that agency's knowledge, has been assigned to that individual by another agency.

The NZTR will use the NHI to identify patients, in a manner consistent with other registries and quality assurance groups. The use of the NHI number is consistent with Schedule 2 of the HIPC, noting that the NZTR is hosted by a DHB.

Appendix A: Brochure about the NZTR