



Major Trauma National Clinical Network

Privacy Framework

NZ Major Trauma Registry

1 July 2016

Final submission to the Office of the Privacy Commissioner

Contents

Letter from Office of the Privacy Commissioner.....2

Overview.....4

Privacy Principles5

 Collection5

 Security7

 Access9

 Retention.....11

Response to Privacy Act Principles 133

Appendix A: Information Sheet for Trauma Patients..... 18

Contact details for further information

Siobhan Isles
National Programme Coordinator
Major Trauma National Clinical Network
Siobhan.isles@nra.health.nz
Mob: 021 578 654

Acknowledgements

The Major Trauma National Clinical Network would like to acknowledge Dr Andrew Kerr and the ANZACS-QI team for their support and provision of background material for this Privacy Framework.

29 June 2016

Siobhan Isles
National Programme Coordinator
Major Trauma National Clinical Network

Dear Siobhan,

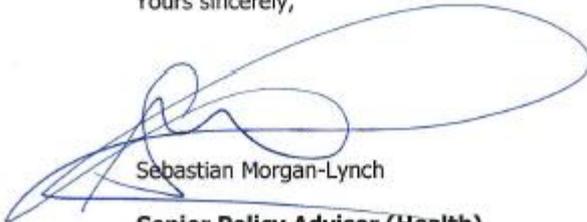
Privacy Framework for the New Zealand Major Trauma Register

Thank you for seeking out views on this Privacy Framework for the New Zealand Major Trauma Registry.

Based on our discussions and having reviewed the '8 July Final for OPC' version of the Framework, we are comfortable with the way this framework sets out the proposed information flows and mitigates potential risks for the clinical information.

We note that the Framework assumes that individual DHB privacy statements will accommodate the proposed uses but have not confirmed that this is the case.

Yours sincerely,



Sebastian Morgan-Lynch

Senior Policy Advisor (Health)

Overview

The NZ Major Trauma Registry (NZ-MTR) is a national registry of people admitted to hospital with major injuries following trauma. It is overseen by the Major Trauma Registry Governance Group that reports to the Major Trauma National Clinical Network (MTNCN).

Trauma injuries and trauma care are difficult to measure and analyse because trauma may involve a large number of medical specialties and does not neatly fit into the diagnosis or procedure-based medical coding systems used in hospitals. Existing systems do not capture all the injuries, nor do they score injuries or produce outcome predictions. The hospital record systems also do not have any information from the pre-hospital setting.

For these reasons it is necessary to establish a national major trauma registry to better understand and improve trauma care in New Zealand hospitals.

Trauma registries are well established in other countries and have been running in individual hospitals in New Zealand for some time.

The NZ-MTR will enrol patients who are 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 and a patient is included with a score of 13 or more.

Information is collected about the mechanism and type of trauma, pre hospital care, emergency department care, injuries, operations, intensive care, and hospital outcome.

This information will be used by the MTNCN and authorised researchers to provide data about the epidemiology of trauma, the initial care, the injury patterns, and the patient outcomes. Its main use will be quality improvement of health care delivery in hospitals. Secondary use will be as a data source for researchers and for linking to other trauma data collections.

The framework for the collection, management and use of health information about identifiable individuals held within NZ-MTR 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, 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.

Reference documents

The following documents are referenced:

1. MTNCN National Minimum Dataset Dictionary 2015
2. MTNCN Data Use Policy 2015
3. Waikato DHB Information Security Policy 2015
4. Waikato DHB Privacy Impact Assessment 2015

These references are available on request from siobhan.isles@nra.health.nz.

Privacy Principles

The following are the privacy principles under which NZ-MTR data is managed.

Collection

What information will be collected?

The New Zealand Major Trauma National Minimum Dataset (NMDS) details the full data set being captured. This reference document is maintained and available on request from siobhan.isles@nra.health.nz.

The data we collect for the NZ-MTR includes the patient's name, date of birth, National Health Index number and address.

The pre-hospital information includes the time and date of the injury, vital signs such as heart rate, and key information about the injury such as whether any protective equipment was being used and what activity was being engaged in when injured. Information about how the patient was transported to hospital is also included.

The hospital information includes the date and time of hospitals the patient was sent to, vital signs, emergency procedures and imaging which were done, intubated and ventilated, whether there were any serious missed injuries, and where the patient was discharged to.

The information we collect is used to score the severity of the patient's injuries using the Injury Severity Scale. Some hospitals collect information on patients whose injuries are scored above 12, other hospitals collect all trauma injury information.

How will information be collected?

Information about the patient and their treatment at the scene and in hospital is collected by clinicians within hospitals to populate the NMDS.

Once collected in hard copy form it is uploaded over the Connected Health Network to the NZ-MTR. The required information is either gathered from the paper medical record or from a hospital electronic patient management system.

Waikato DHB hosts the NZ-MTR as specified in the signed Memorandum of Understanding held between Waikato DHB and the MTNCN, and between the 15 DHBs which are outside of the Midland Region. Different but complimentary agreements are in place with the five Midland Region DHBs.

Why is this information collected?

Information on the patient's care is collected to:

1. Provide individual hospitals with information on trauma admissions, and outcomes.
2. Provide regional and national reporting of hospital trauma activity, care and outcomes.
3. Allow comparative reporting between regions or hospitals
4. Allow epidemiology and research into major trauma incidence, injuries, care and outcome.

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 poster which articulate what patient's need to know about their health information.

In the event a patient specifically requests further information on what happens to their information collected for the NZ-MTR they will be given the opportunity to speak to their health professional and given the Information for Trauma Patients (see Appendix A). They will also be given their DHBs patient information pamphlet which outlines what patients need to know about their health information. Each DHB is required to have information accessible to all patients in line with the Health Information Privacy Code 1994. Specific information about the MTNCN can be provided by the patient's health professional.

Who owns this information?

The information in the NZ-MTR is held (not owned) for privacy purposes by the hospital that has care of the patient at that point in time as part of the existing hospital record. As the host of the NZ-MTR, Waikato DHB is the custodian of all data uploaded to the Registry.

Several hospitals may be involved in a single patient's treatment after a major injury. They each have responsibility for the information collected while the patient is under their care.

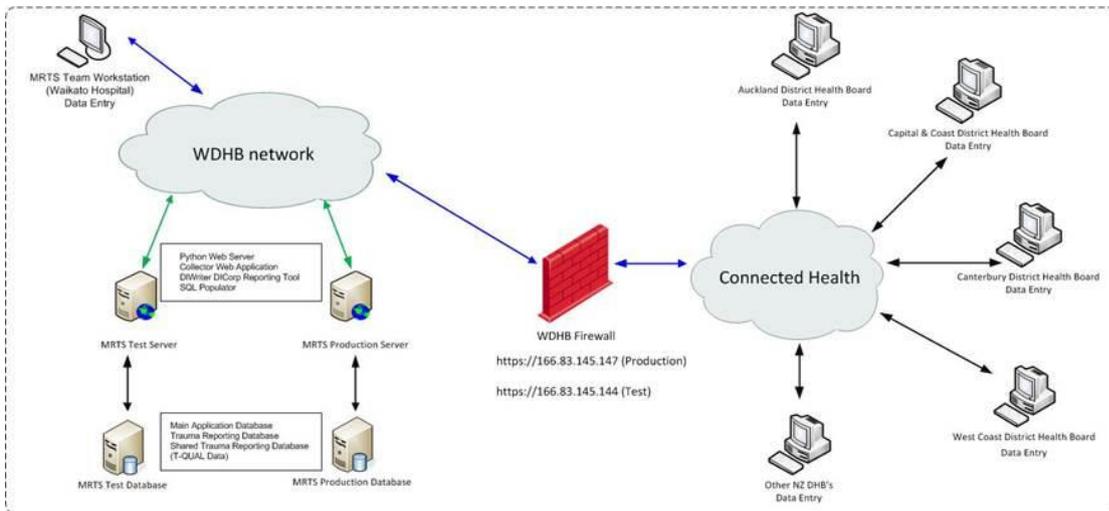
Security

Connected Health Network

The NZ-MTR is run over the Connected Health Network. 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 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.

Information flows across the Connected Health Network to the NZ-MTR



Security of the NZ-MTR technical system falls under the Waikato DHB Information Security Policy.

User identification

All authorised users will have an individual username and password allocated by a system administrator.

All users are assigned to a DHB and to a role which determines their permitted level of access to the NZ-MTR.

Authentication

Access to the NZ-MTR is through individual username and password authentication.

Passwords

In line with the Waikato DHB Information Security Policy, it is recommended passwords are changed every three months and are required to confirm to Waikato DHB's password convention.

Server Location

Application & data resides on Waikato DHB IS environment in a secure data centre, located at Pembroke St, Hamilton, New Zealand.

Data Centre Profile:

Spark Digital Hamilton Data Centre - Aligned to TIA 942 Tier 2 and Uptime Institute standards

- 24 x 7 Spark Digital Managed Data Centre with climate control, diesel generator and UPS power backup.
- 24 x 7 Air-conditioning (HVAC) in a redundant n+1 configuration

Data Centre Security:

- Individual swipe Access card and PIN to prevent unauthorized access
- Electronic monitoring and surveillance of access systems and premises
- 24 x 7 External Closed Circuit (CCTV) monitoring system at entry and within the data centre

The servers are physically located at Spark Digital Data Centre, Level 3 Caro Street Exchange Building, Hamilton, New Zealand.

No information held on the NZ-MTR is transferred outside of New Zealand.

Backup

The MRTS data servers are co-located on a Waikato DHB clinical SQL data cluster with an incremental hourly backup and a full differential daily backup. There is also a full weekend backup.

Access

A relatively small number of users need to access the NZ-MTR. This is likely to be one to two clinicians and/or administrators per DHB.

There are five levels of access:

- Local Access: this enables view/edit/delete access at DHB level only
- Regional Closed: enables view for all DHBs within the region but not edit/delete
- Regional Open: enables view/edit/delete for all DHBs within the region
- National Open: enables view/edit/delete/add for all DHBs. This level of access is held by a small select number of people in the quaternary referral hospitals (Auckland City Hospital, Middlemore Hospital, Christchurch Hospital)
- Administrative: enables view/edit/delete/add for all DHBs nationally. Also enables the addition to certain data points in the registry and can allocate and maintain passwords and permission levels. This level of access is held by the Registry Support Coordinator based at Waikato

As patients get referred from one trauma centre to another, the patients' trauma data is then viewable by multiple DHB and/or Regional entities; however it is only editable by the current treatment facility. This arrangement is subject to local and regional agreements for data sharing.

Reporting and Data Quality Assurance of information held within the NZ-MTR is managed by Waikato DHB as host of the Registry and funded by the MTNCN.

Searching

Patients can be searched for by name or NHI. Other search capability includes by event number, facility, ACC number, injury date, last name first name, DOB, created-by user. They can also be identified by hospital of admission and admission date.

Patient Access

All patients will have the right to access information about them collected in the NZ-MTR on request to their health professional who will follow their DHB's process to provide access to the medical record.

Patients will not be provided with direct access to the NZ-MTR.

Opting out

Following discussion with their health professional and review of the patient information, if a patient wishes to opt-out of the NZ-MTR they can do so. This will be facilitated by the patient's health professional to delete the record and advising the NZ-MTR Helpdesk.

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. Initially, the request will be given to the patient's healthcare professional who will decide whether the request should be actioned.

If deemed the change should be made, the healthcare professional can then refer the request to the NZ-MTR Helpdesk to make the required change. The person who requested the change will be advised when the update has been made by their healthcare professional or their delegate.

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 NZ-MTR setting the change request as provided by the patient and reason for decline.

Audit Log

All submissions of data into NZ-MTR 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 NZ-MTR also has the capability to audit who views a patient record and audits will be undertaken as required.

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 NZ-MTR 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 NZ-MTR.

Use

The MTNCN Data Use Policy has been agreed by the NZ-MTR Governance Group and details the use of data held in the NZ-MTR.

Most individual DHB's only will 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 NZ-MTR 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 NZ-MTR Governance Group or their delegate, before data is released.

In general, data will not be provided from the NZ-MTR to any external research or other external group which could identify patients. 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.

Disclosure

No third parties have access to the data within NZ-MTR directly. Access to the NZ-MTR is only through authorised access, and includes DHB staff with authority to access and Waikato DHB as host of the registry.

Official Information Act requests may be made by members of the public from time to time in relation to the NZ-MTR. Any data released under this Act will be patient anonymised (requests by the patient themselves and will be dealt with under the Privacy Act/Health Information Privacy Code. The NZ-MTR 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 NZ-MTR noting s9(2)(a) allows identifiable information to be withheld in most cases.

Unique Identifier

The NZ-MTR 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.

Inappropriate Access

Inappropriate access to information on the NZ-MTR by any user is considered a serious breach of trust. The NZ-MTR Governance Group Chair (as relevant) 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.

Response to Privacy Act Principles

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 trauma quality assurance activities 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 publically 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) it is not practicable; or*
- (f) the subject would not be identified; or*
- (g) the information will be used for statistical purposes and won't be published.*

The NZ-MTR will generally not collect information directly from patients. It will obtain information from the hospital medical record of the patient as it is not practicable to obtain it directly. On occasion the patient may be asked information that is not available in the notes, such as where the accident was and whether seat belts or other protective devices were used. In some instances it will not be practicable to seek this information.

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 purpose for collecting personal information is clinical and covered by existing collection statements within each DHB. Each DHB has patient information pamphlets and posters which articulate what patient's need to know about their health information.

In the event a patient specifically requests further information on what happens to their information collected as part of the NZ-MTR they will be given the opportunity to speak to their health professional, and be given the Information Sheet for Trauma Patients (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.

Information is obtained from hospital medical records and on occasion and if appropriate, direct from the patient.

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.

Patient information is held in a secure system in the Waikato DHB data centre. The data centre complies with industry standards for network storage.

External (outside Waikato DHB) connections to the data centre will be via the Connected Health Network.

A relatively small number of users will access the NZ-MTR. Users will require authenticated username and password.

Access is logged and can be audited on request.

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 from the Senior Medical Officer who has primary management for the patient.

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.

Information held about a patient is obtained from hospital medical records. Any request for a correction will be submitted to the health practitioners caring the patient, and any correction they make will be updated to the NZ-MTR.

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 be recorded in the comments section of a patient's record in the NZ-MTR.

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 NZ-MTR notes any inaccuracies in the hospital medical record they will inform the team caring for the patient, who will update the record.

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 NZ-MTR 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 MTNCN 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 assurance activities for hospitals and for research purposes following appropriate ethics approval. It is not a clinical application used by hospitals to manage a patient's care.

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 MTNCN Data Use Policy has been agreed by the NZ-MTR Governance Group and details the use of data held in the NZ-MTR.

Aggregate data within the NZ-MTR 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 NZ-MTR Governance Group or their delegate before data is released.

Data will not be provided from the NZ-MTR to any external research or other external group which could identify patients. All data requests will only ever be serviced using unidentifiable patient level, or aggregate data (also non-identifiable).

In exceptional cases, and with ethics and other appropriate approval, 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.

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 NZ-MTR will use the NHI to identify patients, in a manner consistent with other registries and quality assurance groups.

Appendix A:

Information Sheet for Trauma Patients

This information sheet is to inform you about the specific information we collect about you and your care which is entered into the New Zealand Major Trauma Registry (NZ-MTR). This Registry is used to track your journey from the time of your injury until discharge from hospital.

We collect this information to help us understand how we can prevent injuries occurring and where we can improve the quality of care in the pre-hospital and hospital services. It also helps us to compare our performance with other countries such as Australia.

What information is collected?

The data we collect for the NZ-MTR includes your name, date of birth, National Health Index number and address.

The pre-hospital information includes the time and date of the injury, your vital signs such as heart rate, and key information about the injury such as whether any protective equipment was being used and what activity you were doing when injured. Information about how you were transported to hospital is also included.

The hospital information includes the date and time of hospitals you sent to, your vital signs, emergency procedures and imaging which were done, whether you were on a ventilator and for how long, whether there were any serious missed injuries, and where you were discharged to.

The information we collect is used to score the severity of your injuries using the Injury Severity Scale. Some hospitals collect information on patients whose injuries are scored above 12, other hospitals collect all trauma injury information.

Who is responsible for keeping my information safe?

The District Health Board of the hospital you are admitted to is responsible for security around the collection and uploading of information, in line with other health information about you. The Major Trauma National Clinical Network has overall accountability for ensuring all information held in the NZ-MTR is secure.

The NZ-MTR is physically located in secure services located at Waikato District Health Board which hosts the NZ-MTR. Access to the NZ-MTR is restricted to authorised users who require username and password and are clinicians employed by District Health Boards to collect and upload trauma data. There are a limited number of users in each District Health Board.

The NZ-MTR Governance Group is responsible for managing the information which is held in the NZ-MTR. At times external researchers may request information which is held in the NZ-MTR to research aspects of trauma. This research is important to us to show where we should focus our attention to

prevent injuries and improve the quality of our care. The NZ-MTR Governance Group will ensure the appropriate ethics approval is obtained before any data is released, and particularly for any research which requires patient identifiable information.

We will also provide regular reports on aggregate national data. This is data which pools the information in each hospital, and region, and contains no identifiable information.

Can I see my information held in the NZ-MTR?

You will not be able to access the NZ-MTR directly however you may ask for a copy or a summary of your information from your health professional. This may be the doctor or nurse caring for you. You can ask them to explain the information to you if needed. You may request any of your information to be changed, you can discuss this with your health professional to see if this is possible. Any changes made, or not made, will be noted on your record.

Can I opt out of the NZ-MTR?

Yes you may opt out at any time, with no explanation necessary. To opt out inform the doctor or nurse caring for you and they will action your request by informing the NZ-MTR Helpdesk. The request will be actioned as soon as expedient (within business hours).

Where can I go for more information about my rights?

The hospital you are being cared for will be able to provide information about your privacy. Please ask the doctor or nurse who is caring for you.

The Office of the Privacy Commission administers the Privacy Act 1993 and Health Information Privacy Code 1994 and has useful information on its website www.privacy.org.nz.