Midland District Health Boards
Regional Privacy Framework:
Electronic Data

**Purpose**
The purpose of this document is to describe the privacy principles and policy requirements for the supply and use of Midland District Health Boards regional clinical electronic information systems and datasets.

**Author:** Corinne Gower on behalf of the Regional Privacy Group

**Last Updated:** 21 January 2015

**Document Name:** Regional Privacy Framework: Electronic Data

**Version:** V0.14
# Table of Contents

1. INTRODUCTION .................................................................................................................................................................................. 6
2. THE MIDLAND REGION PRIVACY FRAMEWORK ....................................................................................................................................... 8
3. MANAGEMENT ............................................................................................................................................................................................. 10
4. NOTICE .................................................................................................................................................................................................. 12
5. CHOICE AND CONSENT .................................................................................................................................................................................. 13
6. PURPOSE, SOURCE AND MANNER OF PERSONAL INFORMATION COLLECTION .................................................................................................................. 13
7. USE, RETENTION AND DISPOSAL OF PERSONAL INFORMATION ................................................................................................................. 14
8. ACCESS ....................................................................................................................................................................................................... 15
9. DISCLOSURE TO THIRD PARTIES ................................................................................................................................................................. 15
10. SECURITY .................................................................................................................................................................................................. 15
11. QUALITY .................................................................................................................................................................................................. 16
12. MONITORING AND ENFORCEMENT ......................................................................................................................................................... 16
13. COMPLAINTS AND BREACHES ................................................................................................................................................................. 17

Midland District Health Boards Regional Privacy Framework: Electronic Data Draft v0.14

January 2015
## Distribution List

<table>
<thead>
<tr>
<th>Name</th>
<th>Issue Date</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Midland Regional Privacy Group, Midland Region Chief Executives</td>
<td>22/01/2015</td>
<td>0.14</td>
</tr>
</tbody>
</table>

## Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Author</th>
<th>Summary of Changes</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jun to Sept 14</td>
<td>Corinne Gower</td>
<td>Initial Drafts</td>
<td>0.01 to 0.06</td>
</tr>
<tr>
<td>Oct-14</td>
<td>Corinne Gower</td>
<td>Final draft for Regional Consultation</td>
<td>0.07</td>
</tr>
<tr>
<td>Nov-14 to Jan-15</td>
<td>Corinne Gower</td>
<td>Incorporation of regional feedback. Draft finalisation in preparation for CE submission</td>
<td>0.08 to 0.13</td>
</tr>
<tr>
<td>Jan-15</td>
<td>Corinne Gower</td>
<td>Final draft</td>
<td>0.14</td>
</tr>
</tbody>
</table>
## Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clinical Data Repository (CDR)</td>
<td>A database of patient identifiable clinical information such as laboratory results, radiology reports and dispensed medications.</td>
</tr>
<tr>
<td>Clinical Workstation</td>
<td>The electronic information system which presents a patient’s clinical record to the clinician. This retrieves relevant information from multiple sources, and displays this in a single, familiar view. It includes tools to support the clinician in managing a patient. It may be accessed on a range of platforms, including desktop, laptop and tablets.</td>
</tr>
<tr>
<td>eSPACE</td>
<td>A programme of work delivering information systems for health provider organisations supporting patients and clinicians in the Midland region.</td>
</tr>
<tr>
<td>HealthShare (HSL) Ltd</td>
<td>The Midland District Health Boards Shared Services Agency</td>
</tr>
<tr>
<td>Health Information</td>
<td>Information about an identifiable individual including:</td>
</tr>
<tr>
<td></td>
<td>(a) Information about the health of that individual, including their medical history;</td>
</tr>
<tr>
<td></td>
<td>(b) Information about any disabilities that the individual has or had;</td>
</tr>
<tr>
<td></td>
<td>(c) Information about any health services or disability services that are being provided, or have been provided to that individual;</td>
</tr>
<tr>
<td></td>
<td>(d) Information provided by that individual in connection with the donation by that individual, of any body part or any bodily substance or that individual or derived from the testing or examination of any body part, or any bodily substance of that individual; or</td>
</tr>
<tr>
<td></td>
<td>(e) Information about that individual which is collected before or in the course of, and incidental to, the provision of any health services or disability services to that individual.</td>
</tr>
<tr>
<td>Integrated Care Initiatives</td>
<td>Information sharing enablers provided as part the National Health IT Board Integrated Care Initiatives Programme: Shared Care Provider portals (Long Term Conditions, Shared Maternity Record View, Child Action Plan Information System, Whānau Ora Information System) Provider/Clinical Portal, National Child Health Information Platform, Clinical Pathways and eEnrolment).</td>
</tr>
<tr>
<td>Midland District Health Boards</td>
<td>The collective term for the five District Health Boards in the Midland Health Region: Bay of Plenty, Lakes, Tairawhiti, Taranaki and Waikato District Health Boards.</td>
</tr>
<tr>
<td>Midland Regional Clinical Information System Enablers</td>
<td>The clinical information systems and datasets being delivered through HealthShare Programmes.</td>
</tr>
<tr>
<td>Midland Regional Information Platform</td>
<td>The applications and infrastructure being delivered in order to ensure the Midland Region delivers the National Health IT Board Regional Information Platform Priority Programme. Information systems being consolidated in secondary and tertiary healthcare settings include: Clinical Data Repositories / Clinical Workstation; Patient Administration Systems; Imaging/PACS; Clinical support – Labs / Pharmacy; and Continuum of care: eReferrals and eDischarges.</td>
</tr>
<tr>
<td>The Midland Regional Privacy Group (RPG)</td>
<td>An interim group formed in June 2014. The Group was charged with drafting this Framework. The role and future functions of the Group will be discussed and endorsed at a later date.</td>
</tr>
</tbody>
</table>
1. Introduction

The Midland Health Region in the central North Island consists of Bay of Plenty, Lakes, Tairawhiti, Taranaki and Waikato District Health Boards. Each District Health Board (DHB) is accountable for the funding, planning and provision of publicly funded health care services to its district.

Since the introduction of the New Zealand Public Health and Disability (Planning) Regulations in 2011, DHBs have been required to work together in a more integrated way. The Midland District Health Boards have outlined the role to be played by regional electronic clinical information systems and datasets in the Midland District Regional Services Plan (2014/2015)\(^1\).

HealthShare, the Midland DHBs shared services agency\(^2\), is responsible for co-ordinating the delivery of the regional clinical information systems and datasets (Midland Regional Clinical Information System Enablers\(^3\)) to support patients and clinicians across the region. These enablers are needed because:

- Lack of access and integration of health information leads to knowledge gaps which increases risks for patients and clinicians around decision making.
- Disparate health information systems and poor quality health information can lead to adverse patient outcomes.
- The relationship between Information Services and clinical outcomes is not fully recognised when business change is planned. This can lead to ineffective implementation of information systems.
- Poorly integrated health information can lead to inefficient use of time and resources.

The National Health IT Plan Update (2013) has identified Priority Programmes for Information Technology investment\(^4\). DHBs are required to consolidate information systems used in secondary and tertiary settings into regional or national platforms to align with National Health IT Plan targets. ePharmacy is an example of a Regional Clinical Information System that will be used by Midland DHBs Hospital Pharmacy Services.

Midland DHBs will continue to have local information sharing standards and policy applicable to online and paper records. This document is concerned with the principles of health information privacy as they apply to the viewing (online and offline), re-formatting (electronic and paper) and data warehousing of electronic information stored in Midland Regional Information Platforms. The document also discusses regional privacy management and what the region requires from HealthShare programmes, such as eSPACE. Since regional information platforms are evolving The Midland Regional Privacy Framework is expected to be a ‘living document’.

1.1. The Midland eSPACE Programme

The Midland eSPACE Programme has been approved by Midland DHB Chief Executive Officers. eSPACE supports the integration of health information at a regional level and will deliver Midland regional, rather than local, electronic clinical information systems to health provider organisations supporting patients and clinicians. The functions of the electronic clinical information systems are likely to extend beyond traditional hospital boundaries and will be comprised of multiple integrated solutions. Examples of eSPACE information systems include:

- Clinical Workstation: The electronic information system which presents a patient’s clinical record to the clinician. This retrieves relevant information from multiple sources, and displays this in a single, familiar view. It includes tools to support the clinician in managing a patient. It may be accessed on a range of platforms, including desktop, laptop and tablets.
- Clinical Data Repository: A database of patient identifiable clinical information such as medications, laboratory results, radiology reports, care plans, patient letters and discharge summaries. It will provide an up to date, trusted source of patient clinical information and is closely integrated with the Clinical Workstation.

---

\(^1\) See Midland District Health Services Regional Services Plan pages 27 and 72-74. Midland Regional Clinical Information System Enablers is a collective term for a number of information systems that collect information of a clinical nature.

\(^2\) See http://www.healthshare.health.nz/about/healthshare.

\(^3\) Midland Regional Clinical Information System Enablers is the term used throughout this document to describe the clinical information systems and datasets being delivered through HealthShare Programmes.

\(^4\) http://ithealthboard.health.nz/national-health-it-plan
1.2. Safe Trusted Information Access

As we move away from traditional paper health records to increased use of electronic information systems and as information sharing extends beyond existing organisation and information governance boundaries; we need to consider how to best manage regional privacy implications and information assets. The Midland District Health Boards recognise there will continue to be a mix of local, regional and national information systems; operational policy and data governance arrangements.

The eSPACE Programme has developed this document (The Midland Regional Privacy Framework: Electronic Data) and a Regional Information Security Framework which, along with Health Information Governance, underpins the safe, trusted access and use of health information in the Midland DHBs Regional Clinical Information System Enablers.

1.3. Regional Privacy Group

The Midland Regional Privacy Group (RPG) was formed in June 2014. Its Terms of Reference were to:

1. Review current Midland District Health Board Privacy and Information Security Policy and other reference documents to confirm policy alignment and identify policy gaps.
2. Consider which legislation, standards and guidelines are most relevant to regional information sharing.
3. Determine high level privacy business requirements for regional clinical systems enablers.
4. Develop and document a Regional Privacy Framework.
5. Develop additional detailed documentation underpinning the core principles of the Regional Privacy Framework which could be used as direct inputs into the eSPACE Security Framework Group.
6. Identify and document an agreed approach to community and consumer engagement. (Not completed.)

1.4. Privacy Reference Review

The RPG had detailed discussion of privacy requirements applicable to Midland Regional Clinical Information System Enablers and considered the following legislation, standards and guidelines to be relevant to regional privacy:

- The Privacy Act 1993
- The Health Information Privacy Code 1994
- The Code of Rights (Health and Disability Commissioner) 1996
- Professional codes of ethics and conduct
- The Official Information Act 1982
- The Public Records Act 2005
- Connected Health (Health Information Standards Organisation 10037)
- Health Network Code of Practice (SNZ HB 8169:2002)
- Health Information Security Framework (Health Information Standards Organisation 10029)
- Generally Accepted Privacy Principles (2009, American Institute of Certified Public Accountants, Inc. and Canadian Institute of Chartered Accountants)
- Auckland Region DHBs TestSafe Privacy Framework v3.1 (2010, TestSafe)
- Electronic Shared Records: Elements of Trust report (2014, Privacy Commissioner)

---

5 Midland DHB policy and other region privacy frameworks (where available) were analysed in detail. The RPG relied on the legal and professional expertise of its members to discuss applicable legislation and Standards.
1.4.1. Findings

Whilst it was always intended that the focus of information privacy would be broader than DHB Groups\(^6\), because the RPG had prior knowledge and control of existing policy, we have used existing DHB privacy policy as a starting point.

The findings of the privacy reference review are:

Existing Midland DHBs privacy policies are well aligned but because DHBs are at different stages of implementing Midland Regional Clinical Information System Enablers there are policy gaps on data governance and how privacy breaches will be recognised and managed between Midland region stakeholders.

All users of Midland Regional Clinical Information System Enablers and datasets should be made fully aware of their legislative responsibility to adequately protect individual privacy in respect of the way personal information is collected, stored, used, corrected, disclosed and disposed of.

Existing policies may not recognise regional and local dataset relationships\(^7\). Regional datasets may be aggregated copies of local datasets, therefore regional access controls must align with local access controls.

The Generally Accepted Privacy Principles (2009) (GAPP)\(^8\) provided an excellent focal point for the approach the RPG has taken in its consideration of regional privacy matters.

The Midland District Health Boards Regional Privacy Framework should focus on the privacy aspects of regional information system access and sharing to support the eSPACE Programme.

As a result of feedback on earlier drafts of this document, the Group has gained awareness of stakeholder concerns and of other national and local networks considering health information privacy.

2. The Midland Region Privacy Framework

2.1.1. Purpose Statement

The purpose of the Midland Region Privacy Framework is to describe the high level privacy principles and policy requirements for the supply and use of Midland Regional Clinical Information System Enablers to enable patient-centric information to be accessed and shared. Systems should be accessed and information used in a way that engenders confidence and trust and respects the privacy needs of the patient/healthcare consumer, health care providers and participating organisation employees.

2.1.2. Intended Audience

The intended audience of this document is all Midland Regional Clinical Information System Enabler stakeholders. Examples of stakeholders include eSPACE projects and implementers; DHBs, Public Health Units, Primary Health Organisations and primary care practices, independent GPs, private specialists, diagnostic service providers and community based healthcare providers, such as pharmacies and Non-Government Organisations.

It is assumed the reader will have knowledge of the Health Information Privacy Code and refer to the legislation, standards and guidelines listed in section 1.4 (page 7) as required.\(^9\)

---

\(^6\) The Framework recognises there are principles of access to Primary Care data in the context of regional information sharing that are yet to be fully discussed by RPG and eSPACE.

\(^7\) This was observed by the RPG representative from the eSPACE Security Framework Group

\(^8\) The GAPP can be downloaded from [http://www.aicpa.org/INTERESTAREAS/INFORMATIONTECHNOLOGY/RESOURCES/PRIVACY/GENERALLYACCEPTEDPRIVACYPRINCIPLES/Pages/default.aspx](http://www.aicpa.org/INTERESTAREAS/INFORMATIONTECHNOLOGY/RESOURCES/PRIVACY/GENERALLYACCEPTEDPRIVACYPRINCIPLES/Pages/default.aspx)

\(^9\) The Framework recognises there is parallel Midland Regional Information Security work stream and the Health Information Governance Expert Advisory Group (HIGEAG) is developing a Health information Governance Framework (due to be released mid 2015).
2.1.3. **Scope**

The National Health IT Plan describes the work that needs to be done to achieve the Government’s eHealth vision that all New Zealanders will have electronic access to their own core health information. The Midland Regional Privacy Framework applies to the people who are using and sharing clinical information by way of access to Midland Regional Clinical Information System Enablers. The patient is not expected to have direct access to these systems. It is recognised that in the future information may be exposed to a patient through self-care or shared care portals and information sent back to primary care is discoverable by the patient.

The Midland Region Privacy Framework is applicable to:

- Midland Regional Clinical Information System Enabler users and sharers of health information, such as employees, contractors, Board members, persons working on behalf of agencies such as volunteers, students and agency contractors.
- All stages of the information system and paper records lifecycle which involve personal information. Examples of scope include the design, acquisition, development, testing, training, implementation, configuration, modification and management of:
  - Infrastructure, Systems, Applications, Web sites, Procedures, Products and services, Databases and information repositories, Mobile computing and other similar electronic devices.

2.2. **The Ten Generally Accepted Information Privacy Principles**

The Framework is structured around ten generally accepted information privacy principles, which are discussed in turn: ¹⁰

1. There is management accountability for privacy policies and procedures.
2. Individuals should be notified about the existence and purpose of information sharing.
3. Individuals should be notified of any choice and consent options.
4. The purpose of personal information collection should be clear.
5. Procedures should be in place to support the appropriate and secure use, retention, and disposal of personal information.
6. The provisions for an individual to access personal information held about them should be clear.
7. The process for disclosure of personal information to third parties should be clear.
8. Security measures should be in place to protect privacy.
9. Quality assurance measures should be in place to preserve the integrity and security of personal information.
10. Procedures and controls should be in place to monitor and enforce compliance with privacy policy.

¹⁰ *Generally Accepted Privacy Principles* (2009, American Institute of Certified Public Accountants, Inc. and Canadian Institute of Chartered Accountants) p. 7.
3. Management

**Principle 1: There is management accountability for privacy policies and procedures.**

Participating organisations should be confident that systems are in place to support trusted access and safe information sharing. This principle recognises the needs for a common approach and management accountability for the development of regional privacy policies and supporting business processes.

The eSPACE governance structure is approved by Midland CEOs and reflects the ongoing governance of privacy and security in the Midland region.

![Figure 1 eSPACE Governance Structure modified to include Privacy and Security](image)

The HealthShare Chief Executive Officer is accountable for delivery of the Midland Region Information Strategic Plan and regional IS services in line with Midland DHB Chief Executive Officer agreement and business case approvals.

The Midland Information Services Executive (eSpace Programme Board and eSpace Advisory Board) advises the HealthShare Chief Executive Officer and monitors portfolio alignment of the eSpace programme.

The Midland Information Services Leadership Team provides expert advice into the Strategic Plan delivery and is responsible for the effectiveness of regional services. The team is advised by DHB Information Service teams and Regional Information Service Groups.

The eSPACE Programme Board, reporting to the HealthShare Chief Executive Officer, provides Programme governance and ensures delivery of the agreed eSPACE Work Programme.

The role of the Midland eSPACE Advisory Group is to provide advice and recommendations on key aspects of the programme to support and enhance the decision making processes of the eSPACE Programme Board. The group has strong linkages into the regional clinical networks and Regional Service Plan governance groups.

The Midland Regional Privacy Group (RPG) is an interim group charged at this point with drafting the framework. Its role and future functions will be discussed and endorsed by The Midland Information Services Leadership Team at a later date.

The RPG’s recommendations for management of Midland regional privacy at the DHB and participating organisation level are now discussed.
3.1 Review and Approval of Privacy Policy

Regional privacy policy will be reviewed and approved by the eSPACE Programme Board, Midland IS Leadership Team and Midland Regional Privacy Group.

3.2 Role of Privacy Officer

All participating organisations with access to Midland Regional Clinical Information System Enablers will have a nominated Privacy Officer. This is a functional role and the role holder can hold other responsibilities. The nominated Privacy Officer should be available for consultation on regional privacy matters.

3.3 Role of Organisation Line Management

Line managers in participating organisations with access to Midland Regional Clinical Information System Enablers are required to ensure staff receive health information privacy training and comply with regional information system standard operating procedures and privacy policy.

3.4 Midland Regional Systems Asset Register

HealthShare will maintain a Midland Regional Clinical Information System Enablers Asset Register. The Register will include details of the software version and upgrade patches applied to all environments of the Midland Regional Clinical Information Systems Enablers.

The Asset Register will serve as a management reference document for participating organisations who wish to confirm these details.

3.5 Risk Assessment

The Regional Privacy Group should ensure an annual risk assessment of Midland Regional Clinical Information System Enablers is undertaken. Completion of the assessment can be delegated to a third party (DHB or independent vendor) and should support the principles and guidelines outlined in the ISO Risk Management Standard (31000, 2009). The purpose of the risk assessment is to establish a risk baseline, from which new or changed risks to personal information can be identified and responses to such risks can be developed.

3.6 Infrastructure and Systems Management

Project documentation, Privacy Impact Assessments and participating organisation contracts should address who has made management decisions about how Midland Regional Clinical Information System Enabler have been configured. The rollout of new and major upgrades to support the eSPACE Programme and Regional Information Platforms should involve the documentation and review of a Privacy Impact Assessment and should follow appropriate and auditable change management processes.

Projects implementing or upgrading Midland Regional Clinical Information System Enablers implementation/upgrade should carefully consider the appropriateness of the use of personally identifiable health information in application development, test, training and pre-production environments. The eSPACE Programme Board and Privacy Impact Assessments should fully assess any privacy risk pertaining to personal health information data held in non-production environments.

Personal information must be appropriately protected when information is migrated from old to new or changed systems.

Emergency changes required to maintain the same level of protection of personal information may be documented/approved on an after-the-fact basis.

---

11 The Register will detail eSPACE Regional assets only. DHBs will remain responsible for maintaining local asset registers.
12 Including system components
3.8 Privacy Awareness and Training

A Regional Privacy Awareness training program, including training on the Health Information Privacy Code and regional privacy policies will be provided to Midland Regional Clinical Information System Enabler users and eSPACE Programme project personnel. This program should ideally be electronic; completion of training should be a condition of system access, be ongoing and completed within an agreed timeframe. The details of the regional training program will require endorsement and as such will be confirmed at a later date.

HR staff will also need to receive training on privacy policy and system operational procedures in order to support the training program and enforce any privacy breach sanctions.

Training and awareness courses will be regularly updated to reflect regional privacy requirements. Where possible, privacy training registers will be maintained.

3.9 Privacy Incident and Breach Management

Midland DHBs will have procedures for the identification, management, and resolution of privacy incidents and breaches associated with Midland Regional Clinical Information System Enablers access and use (see Section 13 for further discussion).

4. Notice

Principle 2: Individuals should be notified about the existence and purpose of information sharing.

Participating organisations must publicly notify patients and staff that health information is being shared regionally and how this is being done.

Relevant health professionals should also take reasonable steps to notify their patients about regional information sharing. Ideally, standard public notices will be used ensuring that patients receive consistent information.

The Regional Privacy Group will develop standard public notices which will include the following information:

a. The type of personal information, the sources of such information, and purposes for which it is collected and whether collection is a legal requirement.

b. The consequences, if any, of not providing the requested information.

4.1 Provision of Notice

Notices should be readily accessible and provided in a timely manner to enable individuals to decide whether or not to submit personal information. A range of communication methods in multiple languages should be considered. The needs of patients with visual impairment and literacy issues should be addressed.

Written notices should be in plain and simple language, be appropriately labelled, easy to see and clearly dated. Notices may be linked to or displayed on web sites and be available at points of data collection.

4.2 Scope of Activities covered

Notices should describe situations in which personal information can be disclosed, such as in a medical emergency, when allowed or required by law and the practices related to the sharing of any personal information with third parties, including the reasons and identifying third parties to whom personal information is disclosed.

4.3 Information Retrieval Assumptions

The users of information held in Midland Regional Clinical Information System Enablers must have reasonable grounds for believing that the patient has been informed about information sharing practices, and that notification practices and methods have been followed.
5. Choice and Consent

Principle 3: Individuals should be notified of any choice and consent options.

While privacy law in New Zealand is based on purpose of information collection, it is recognised individuals should be offered choice and consent regarding regional information sharing.

Individuals need to know what choice and consent options are available to them in respect of personal information collection, use, and disclosure to third parties.

Once obtained, consent is not required for every use of health information. Health care providers do not have to obtain consent if it is not reasonably practicable or would prejudice the interests or safety of the patient and others.

5.1 Consent Options

The extent of choice and consent options for regional information systems will depend on the functional capability of the system. Where practical, an individual’s preferences should be indicated in the information system and consent history should be auditable. The timeframes and conditions, such as legal or contractual, under which consent may be withdrawn should be reasonable and clear.

Consent can be implicit: inferred as a result of a person’s silence or inaction; or explicit: a person is given a clear option to agree or disagree.

Where information sharing consent options are offered to an individual, there is the option to opt on or opt off:

- Opt on – the individual is given the option to give consent to regional information sharing, but if they do not clearly give consent, information will not be shared.
- Opt off – the individual is given the option to decline consent to regional information sharing, but if they do not clearly decline consent, information will be shared.

5.2 Consequences of Denying or Withdrawing Consent

When personal information is collected, individuals should be informed of the consequences of refusing to provide personal information. The processes for denying or withdrawing consent to information sharing should be detailed in public notices. For example:

“Call [Telephone Number] to restrict the sharing of your records.”

The consequences of opting-out (e.g. that certain kinds of care may be made more difficult or that the patient may be put at increased risk) should be stated in a clear but not alarmist way. For example:

“If you opt out of regional information system sharing, health professionals caring for you may not immediately have information they need to provide the best and safest care possible. If you are thinking of opting off, please discuss your options with your healthcare provider or the person you speak to when you call the freephone number.”

6. Purpose, Source and Manner of Personal Information Collection

Principle 4: The purpose of personal information collection should be clear.

Health information is collected primarily to help in the care of the individual. Secondary purposes include system improvement, teaching, reporting to funders and audit / outcome research.

Participating organisations are required to have privacy policies that address the collection of personal information and address Rules 1-4 of the Health Information Privacy Code.

---

14 Options will often depend on the functional capability of an information system; whether consent can be electronically recorded at a patient or event level and consent preferences can be managed by the system.
6.1 Purpose
All personal information collected in Midland Regional Clinical Information System Enablers must be needed for a lawful purpose. Privacy Notices and Privacy Impact Assessments should describe the types of personal information collected, including the mechanism of data transfer, to a level that is appropriate for their intended audiences.

6.2 Source of Information
Rule 2 of the Health Information Privacy Code requires that health information be collected directly from the service user. This is the responsibility of the agency collecting the information. Retrieving information from a Midland Regional Clinical Information System Enabler may be a deviation from this rule. As such, clinical staff need to be assured that one of the following circumstances is met when using regional information:

- That the patient or their representative has consented to the use of the information;
- The patient is not able to give their consent; or
- Failure to consult the record would prejudice the interests of the patient or anyone else’s safety.

6.3 Method of Collection
Methods of collecting personal information should be explicit. It is a requirement that all collecting agencies will comply with the Health Information Privacy Code and that personal information is obtained (a) without intimidation or deception, and (b) lawfully.

Unsolicited information must be recorded in a manner that identifies the source, how information can be used and the accuracy of unsolicited information should be verified before it is used.

7. Use, Retention and Disposal of Personal Information

Principle 5: Procedures should be in place to support the appropriate and secure use, retention, and disposal of personal information.

The Framework adopts Health Information Privacy Code Principles 9, 10 and 11.

7.1 Use
Personal information may not be used for another purpose without the knowledge and consent of the person concerned.

Midland Region Clinical Information System Enablers should be used only for legitimate business purposes or approved use. These uses and any specific requirements for handling personal information should be communicated to third parties to whom personal information is disclosed.

7.2 Retention
Personal information should not be kept for longer than it is required for its purpose. Retention times will be documented in the Midland Regional Clinical Information System Enablers Standard Operating Procedures. Personal information should not be kept beyond the standard retention time unless a justified business or legal reason for doing so exists.

Where data is archived or kept for historical purposes, consideration should be given to storage in an open format, and of the ability to read and retrieve in the future if required.

7.3 Disposal
The RPG recognises it is difficult to ensure complete removal of segments of information, (including information in archived and backed up copies). Midland DHBs policy on disposal of records in Midland Regional Clinical Information System Enablers will require careful thought and consideration.

Personal information should be disposed of, or destroyed in a manner that prevents its loss, theft, misuse, or unauthorised access. Disposal should be in accordance with relevant legislation, such as the Public Records Act (2005), General Disposal Authority and the Retention of Health Information Regulations.
The process for disposal of personal information in Midland Regional Clinical Information System Enablers will be detailed in Standard Operating Procedures.

Where data is archived or kept for historical purposes, consideration should be given to storage in an open format, and of the ability to read and retrieve in the future if required.

8. Access

Principle 6: The provisions for an individual to access personal information held about them should be clear.

Rule 6 of the Health Information Privacy Code provides all individuals have the right to request access to their health information. Health information can only be withheld on limited grounds. Public notices will inform individuals how to access their health information, expected timeframes for response and the process for complaints or disputes.

Information may need to be “vetted” before it is copied and sent to a requestor. Vetting maintains confidentiality and ensures other individuals’ privacy is not unnecessarily interfered with.

The identity of a requestor should also be authenticated before access to information is given. If access is denied, the reasons for denial should be outlined to an individual. A record of denial and unresolved complaints and disputes should be recorded. Partial access to information may also be permitted.

Rule 7 of the Health Information Privacy Code provides that the person concerned has the right to request correction of their information and to request that there be attached to the information a statement of the correction sought but not made. Decisions on requests must be made as soon as reasonably practicable and not later than 20 working days after the receipt of the request.

If correction is not possible or appropriate, a note that a request to correct information was made is attached to that part of the record to which it applies, and the person notified accordingly. If practical and economically feasible to do so, updated or corrected information is provided to third parties that previously were provided with the individual’s personal information.

9. Disclosure to third parties

Principle 7: The process for disclosure of personal information to third parties should be clear.

The Framework endorses Health Information Privacy Code Principle 11 that personal information held in Midland Regional Clinical Information System Enablers can only be disclosed to third parties with the consent of the individual concerned unless disclosure without consent is required for a legitimate purpose or by law.

10. Security

Principle 8: Security measures should be in place to protect privacy.

Midland Regional Clinical Information System Enabler users should be aware and comply with the security measures in place to protect the privacy of an individual’s personal information when they use a system. Personal information should be also be protected from unauthorized access when:

- Transmitted by mail or other physical means
- Stored on portable media or devices

The RPG’s information security business requirements are also addressed in the Midland DHBs Regional Security Framework which addresses in detail:

- Risk assessment and treatment
- Security policy
- Organisation of information security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development, and maintenance
- Information security incident management
- Business continuity management

11. Quality

**Principle 9: Quality assurance measures should be in place to preserve the integrity and security of personal information.**

The Framework supports Health Information Privacy Code Principle 8 that reasonable steps are taken to ensure the accuracy of information is verified before it is used.

In particular, Midland Regional Clinical Information System Enabler users should be advised of any loss of information or data integrity arising from data migration into Midland Regional Clinical Information System Enablers.

Midland Regional Clinical Information System Enablers Standard Operating Procedures should describe the frequency of assurance checks and how data quality issues should be identified and addressed. For example, an Midland Regional Clinical Information System Enablers might support regional information sharing by allowing system users to record the date information was verified and displaying details, including the verifying organisation and user, when information is reviewed.

12. Monitoring and Enforcement

**Principle 10: There are procedures and controls in place to monitor and enforce compliance with privacy policy.**

Midland DHBs will have systems and procedures in place to monitor use of and compliance with Midland Regional Clinical Information System Enablers Standard Operating Procedures and privacy policy.

Examples of the types of system and procedures controls in place to monitor and enforce compliance include:

- Notifying employees of the need to report privacy breaches and security vulnerabilities in a timely manner.
- Documenting instances of noncompliance with privacy policies and procedures.
- Monitoring the resolution of security vulnerabilities and privacy breaches to ensure appropriate corrective measures are taken on a timely basis.
- Following processes to ensure employees and others are disciplined, as appropriate, when they cause privacy incidents or breaches (see Complaints and Breaches (below)).
- Mitigating, to the extent practicable, any harm caused by the use or disclosure of personal information by a third party in violation of the entity’s privacy policies and procedures (for example, notify affected individuals, attempt to recover information disclosed to others).

The results of monitoring and enforcement activities will be reported to the Information Services Leadership Team. If problems are identified, remediation plans will be developed and implemented.
13. Complaints and Breaches

Any complaints related to information contained within Midland Regional Clinical Information System Enablers should be directed to the relevant Midland DHBs Privacy Officer who will then refer the complaint to the appropriate PHO, healthcare professional or the provider's employer, depending on where the alleged breach occurred.

The general procedure for dealing with a complaint or an alleged breach is as follows:

13.1 Acknowledgement

The Privacy Officer or appropriate delegate, on receiving a complaint or breach must:

- Contact the person making the complaint in writing, within 10 working days of learning about the complaint or breach, and
- Inform the complainant of any relevant internal and external complaint procedures, and of the action that will be taken within 10 working days.

13.2 Investigation

As soon as practicable after a complaint is accepted, the DHB Privacy Officer must inform the person or their employer of the complaint or breach of what has been alleged.

The privacy officer for this healthcare professional must inform the complainant of the steps proposed to be taken to resolve the complaint or breach, and also that the complainant has the right to contact the Privacy Commissioner.

13.3 No Investigation

If the privacy officer for the healthcare professional decides not to accept a complaint or that a breach has occurred, on the basis that none of the terms of the Health Information Privacy Code or relevant Midland Regional Clinical Information System Enablers privacy have been breached, then as soon as reasonably practicable they must inform the complainant of the reasons for the decision, and the right to contact the Privacy Commissioner regarding the decision. The privacy officer must also advise the relevant governance group.

13.4 Inappropriate Access

Inappropriate access to information in a Midland Regional Clinical Information System Enablers by a staff member, contractor, volunteer or student will generally be considered a serious breach of trust. Midland DHBs will take action, in accordance with employment law, due process and natural justice, which may include disciplinary action, removal of access privileges and referral to a relevant professional authority. Midland DHBs will act in a manner consistent with protecting the integrity and security of a Midland Regional Clinical Information System Enablers.
## Appendix 1: Initial Schedule of Groups Consulted

The following groups have been consulted in along with a number of other stakeholders the preparation of this document:

<table>
<thead>
<tr>
<th>Group</th>
<th>Person</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office of the Privacy Commissioner</td>
<td>Senior Policy Advisor (Health), Sebastian Morgan-Lynch</td>
</tr>
<tr>
<td>National Health Board</td>
<td>Lucy Curtis, Senior Policy Advisor</td>
</tr>
<tr>
<td>National Health IT Board Consumer Panel</td>
<td>Chair, Stephanie Fletcher, Sheldon Ngatai – TDHB Consumer Representative.</td>
</tr>
<tr>
<td>eSPACE Programme Board</td>
<td>Midland DHB Representatives, Orion &amp; Sysmex Vendor representation</td>
</tr>
<tr>
<td>eSPACE Advisory Board</td>
<td>Midland DHB Representatives, Primary Care</td>
</tr>
<tr>
<td>Information Services Leadership Team</td>
<td>Midland DHB CIO Representatives, HealthShare Representatives.</td>
</tr>
</tbody>
</table>