

**RGPG & Lakes DHB – Rotorua Hospital
Emergency Department Regional Project:
Access to Enrolled Patient Information for
Treatment Providers: Phase II**

Privacy Impact Assessment Report
Version 1.1



VERSION	DATE	DESCRIPTION	AUTHOR
0.1-0.2	30/11/12	Initial draft versions	R. Lepa
0.3	18/12/12	Update following internal review	R. Lepa
0.4	16/01/13	Incorporates review feedback from Office of the Privacy Commissioner	R. Lepa
1.0	22/01/13	Update to release status	R. Lepa
1.1	12/06/13	Statement regarding confidential information leaving the practice amended to reflect updated information flow diagram. Pages 5-6	R. Lepa



© RGPG Ltd, 2012. All rights reserved.

No part of this document may be copied or distributed in any form without the written permission of RGPG.

TABLE OF CONTENTS

1	Introduction & Overview	4
2	Project Scope & Information Flows	5
3	Health Information Privacy Rules	7
3.1	Purpose of collection of health information	7
3.2	Source of health information	7
3.3	Collection of health information from the individual	7
3.4	Manner of collection of health information.....	8
3.5	Storage and security of health information	8
3.6	Access to personal health information	10
3.7	Correction of health information	10
3.8	Accuracy of health information to be checked before use	10
3.9	Retention of health information	11
3.10	Limits on the use of health information.....	11
3.11	Limits on disclosure of health information	11
3.12	Unique identifiers.....	12
4	Privacy Risk Assessment	12
5	Privacy Enhancing Responses / Compliance Mechanisms.....	18
6	Conclusion	21
7	Appendices	24
7.1	RGPG PrimeWise Individual User Agreement	24
7.2	RGPG Information Security and Confidentiality Policy	25
7.3	Participating Practice Agreement	27
7.4	Enrolment form template (correct as at July 2012).	29
7.5	Waiting Room Health Information Poster.....	31
7.6	Sample Information Leaflet for Patients	32
7.7	Break the Glass Policy	33

1 INTRODUCTION & OVERVIEW

In 2009 RGPG Limited (RGPG) prepared a proposal for the Lakes District Health Board (LDHB) Rotorua Hospital After Hours/ASH Reference Group that was accepted by this group, and subsequently by the Ministry of Health for funding.

The proposal entailed two phases involving the establishment of a link to PrimeWise (previously known as NZHealthTec) for Rotorua Hospital Emergency Department (RHED) staff to view agreed subsets of information available on PrimeWise. The project was named the “**ED Interface with Primary Care**” project.

PrimeWise is a primary care knowledge management and healthcare provider technology platform, designed, hosted, and maintained by RGPG. All general practices in the Rotorua district are connected to PrimeWise, and individually are the owners of the practice databases hosted within PrimeWise.

Phase One of the project linked RHED administration staff with patient demographic, practice and doctor enrolment details with the intention that these staff:

- have access to up-to-date address and doctor details and can utilise this in patient admission and discharge procedures;
- can identify locally-resident patients who are not enrolled with any doctor, and provide information and support for these patients to be linked into primary care.

During the setup of Phase One, a comprehensive Privacy Impact Assessment (PIA) was completed and reviewed by the Privacy Commission in May 2011.

The access to patient demographic details via PrimeWise was made possible through the private business decision of general practices, to host their practice information on PrimeWise, and the independent decision of these practices to enable third parties to view an agreed subset of this information from a consolidated webview.

The electronic software and system requirements needed to enable a data view to PrimeWise for RHED staff was designed, implemented and provided by RGPG. RGPG monitors the on-going linkage to patient information by RHED and supports the on-going facilitation of the necessary agreements from PrimeWise database owners to access this information. This includes monitoring every time a record is accessed, which tags each view with the User, time, and date that the information was viewed.

The interface went live in June 2011 and is currently being utilised at RHED.

Phase Two of the project is described as expanding the current consolidated webview of demographic and doctor enrolment details, at the primary-secondary interface, to include relevant clinical information.

The purpose of this PIA is to comprehensively evaluate Phase Two with regards to individual privacy concerns, in order to ensure that the project complies with the New Zealand Health Information Privacy Rules. Evaluation will include assessing any impacts upon individual privacy that Phase Two of this project might generate; and how any negative impacts on individual privacy may be addressed and overcome.

This PIA will be circulated to appropriate parties within RGPG, PrimeWise Users, and LDHB for review prior to confirming approval for the next stage of Phase Two to proceed i.e. the implementation of the data view link for systems testing.

This assessment is completed based on the guidelines of the Office of the Privacy Commissioner as detailed in the publication ‘Privacy Impact Assessment Handbook’ (2007). The Office of the Privacy Commissioner’s ‘Health Information Privacy Code 1994: Revised Edition’ (2008) and The Privacy Act 1993 are also referred to in the writing of this report.

The final document will be released and made available as a public document.

2 PROJECT SCOPE & INFORMATION FLOWS

- Currently Rotorua general practices use PrimeWise, along with other health records management applications, to manage and store their patients' individual health and demographical information. The purposes of collecting and retaining this information from individual patients include:
 - Facilitating efficient and effective service and care delivery;
 - Enabling monitoring of health status and follow up care to enrolled patients;
 - Allowing evaluation of the care provided to patients;
 - Providing for the retrieval of data for research and management purposes;
 - Meeting legislative requirements for the provision of information to the New Zealand Health Information Service (NZHIS);
 - Meeting Ministry of Health and other contractual requirements.
- The main deliverable of this project is that RGPG will build and implement a customised data view for RHED staff; presenting a clinical subset of individual patient information contained in PrimeWise. The proposed clinical subset includes:

- Problem Lists (diagnoses and allergies)
- Medications (usual medications and acute prescriptions from last 90 days)
- Recent Contacts/Encounters (practice visits) limited to a maximum of the previous 90 days.

- This clinical subset of patients' individual data received Rotorua Area Primary Health Services (RAPHS) Clinical Leader endorsement on 11th September 2012.
- Patient information will only be available for those patients who are enrolled¹ with a general practice participating in this project and who have consented to their information being viewed at RHED.
- Under the proposed project, there are no changes to the existing way that individual health information is collected and obtained by general practices. There will be a change in how information is stored. Once information reaches PrimeWise, the clinical subset (defined above), will be sent to a Patient Information (Pat-Info) database (see following information flow diagram).

Confidentiality Flag

Current functionality within practice management systems (e.g. Medtech and Profile) allows individual data items to be marked as "confidential". The confidentiality flag is generally used by general practices to mark those items that are particularly sensitive so that they may only be shared with other specifically "trusted" health professionals within the practice.

It is proposed that this flag be used to provide a level of granularity around what information about each patient is able to be viewed by authenticated RHED clinicians. By marking individual items as "confidential", those particular items would not be visible outside of the patient's general practice, while the remainder of the patient record would.

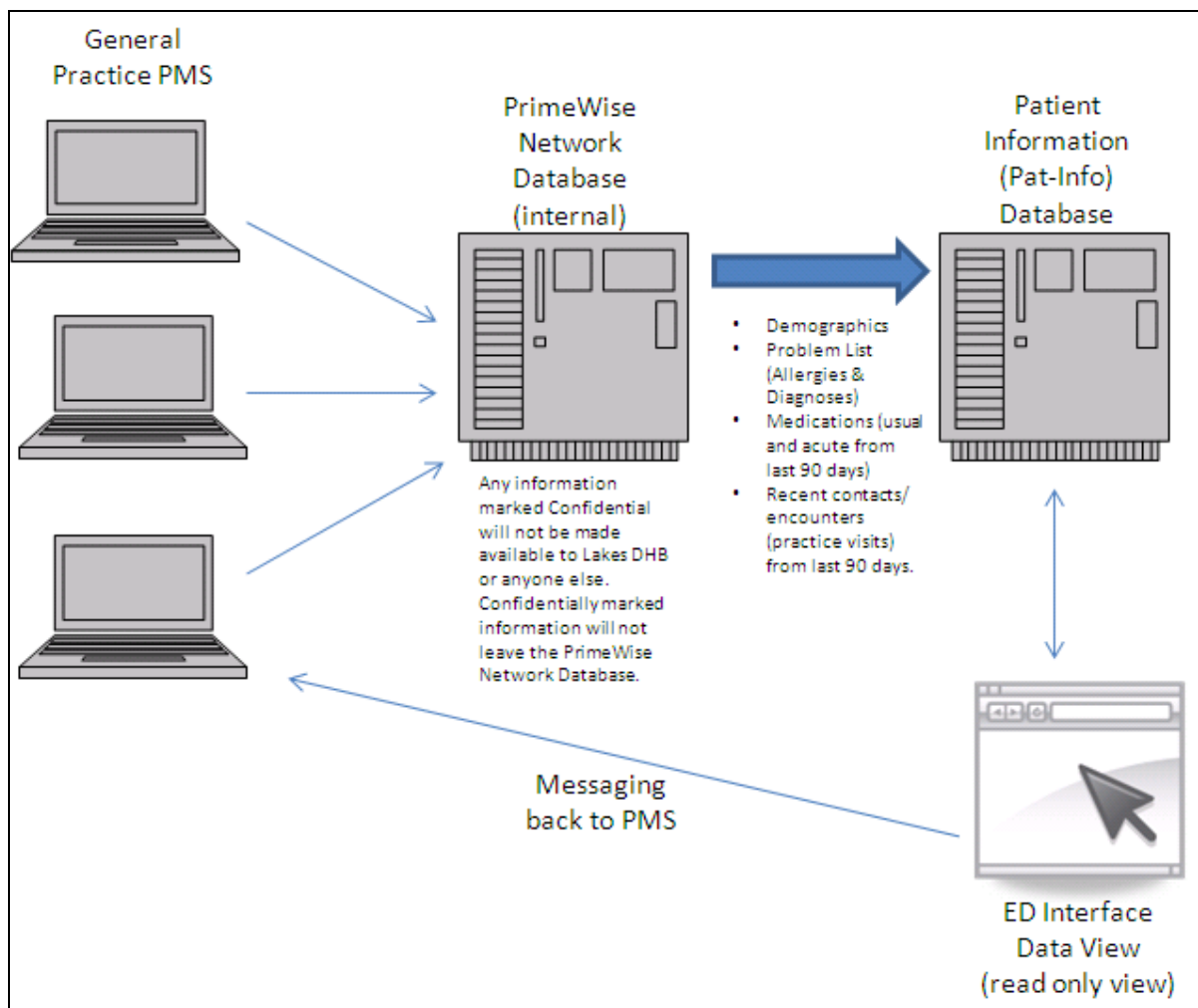
~~Whilst information flagged as confidential will be excluded from all information exported from practice management systems (e.g. Medtech and Profile), the information could still be disclosed by the patient during standard history taking methodologies.~~ Information flagged as confidential could still be disclosed by the patient during standard history taking methodologies. The key point is that the 'control' over who they disclose their sensitive information to, is with the patient.

- Access to the Pat-Info database will be granted to named individuals agreed by LDHB and RGPG. Access will be on an individual User basis. Each User must have unique access credentials and these will be supplied by RGPG.
- Different levels of access will be incorporated to distinguish between different staff roles i.e. administration staff will not have access to clinical information.

¹ Enrolled status means practice PMS system records that state the patient is enrolled with Health Rotorua PHO at last extract date.

- Access to the Pat-Info database will be granted subject to agreed individuals signing and complying with the terms of:
 - (i) the PrimeWise Individual User Agreement (Appendix 1),
 - (ii) the RGPG Information, Security and Confidentiality Policy (Appendix 2).
- Authorised staff members from RHED will not be able to add, modify, remove or alter data from the Pat-Info database in any way – this project would offer them a read only view of the information. The two-way arrow from ED to the Pat-Info database (shown in the following diagram), is to indicate the logging of all successful and unsuccessful access attempts, for auditing purposes. In addition, an automated message will be sent to the patient's general practice to notify that their information had been accessed by RHED.
- Information contained within PrimeWise can only be accessed with the explicit permission of the general practice owner, for an agreed purpose and compliant with the Health Information Privacy Rules, as outlined in the Participating Practice Agreement (Appendix 3).
- Following completion of the PIA, and once the data view has been developed and tested satisfactorily by RGPG, the data view will 'go live' for RHED staff.
- Access to the data view will be via an existing RGPG-LDHB secure private IP connection. RGPG will give all reasonable assistance to LDHB through their service provider to ensure that the integrity, safety and risk mitigation of this link is maintained.
- The following diagram illustrates information flows related to this project:

Information Flows



3 HEALTH INFORMATION PRIVACY RULES

This section will examine the scope of the project against the twelve rules of the Health Information Privacy Code.

3.1 Purpose of collection of health information

Health information must not be collected by any health agency unless: the information is collected for a lawful purpose connected with a function or activity of the health agency and the collection of the information is necessary for that purpose.

Provision of health information by RGPG to RHED serves several lawful purposes connected with the function and activity of both primary and secondary care and treatment of that patient. To summarise:

The purpose for enabling the access to a view of clinical information is to enhance patient safety and care in unscheduled consultations when their general practice is closed. Many patients have difficulty remembering all their medications or pronouncing drug names, especially when ill or confused. By accessing primary care clinical records potential benefits include (but are not limited to):

- more efficient assessment;
- reduced drug interaction;
- reduced adverse reactions; and
- reduced duplicate prescribing rates.

Additionally, the information set provided is restricted to only the information necessary for the purpose of providing emergency clinical care.

3.2 Source of health information

Where a health agency collects health information, the health agency must collect the information directly from the individual concerned unless a relevant exception (such as the individual's representative) applies.

The information view enabled by RGPG to RHED under this project is sourced directly from the Pat-Info database. The source of information stored in the database has been obtained directly from the individual patients and their primary treatment providers.

Presently, when a patient enrolls with or presents to a general practice in Rotorua, their demographic and clinical information is entered into the practice database by practice staff, relevant to their role within the practice. Likewise, when patient details change, the practice database is updated by practice staff to reflect this information.

3.3 Collection of health information from the individual

Where a health agency collects health information directly from the individual concerned, or from the individual's representative, the health agency must take such steps as are, in the circumstances, reasonable to ensure that the individual concerned (and the representative if collection is from the representative) is aware of:

- a) the fact that the information is being collected;
- b) the purpose for which the information is being collected;
- c) the intended recipients of the information;
- d) the name and address of -
 - the health agency that is collecting the information; and
 - the agency that will hold the information;
- e) whether or not the supply of the information is voluntary or mandatory and if mandatory the particular law under which it is required;
- f) the consequences (if any) for that individual if all or any part of the requested information is not

- provided;*
g) *the rights of access to, and correction of, health information.*

When enrolling at their general practice, a consent form (complete with explanation as to purpose and limitations) to collect, obtain, retain, store and share health information with other health professionals and agencies involved in their treatment or care is signed by the individual patient (Appendix 4). RHED would be considered an agency involved in care or treatment of that patient, but in the interest of transparency and best practice procedures, the patient's auditable consent for accessing this information will be sought during the course of the admission process.

Patients would be advised via posters in their general practice and RHED waiting rooms (Appendix 5), information leaflets (Appendix 6), and via direct consultation with general practice staff, that their clinical information may be viewable by authorised healthcare professionals at RHED (from an agreed date), they will be able to request to have confidential information withheld, and that on presentation to RHED, patients will have the option of sharing or not their health information. Explicit consent would not be required if the patient was unable to give their consent (e.g. unconscious) and the information was believed to be clinically relevant/vital to ensure appropriate care was delivered, in accordance with provisions set out in the Health Information Privacy Code 1994 and the RGPG Break the Glass Policy (Appendix 7).

There will be no consequences placed upon the individual who does not give consent for RHED clinical staff to access their information within the confines of this project. They will receive the same level of care and treatment that they would otherwise receive, however it may take treatment providers longer to take a presenting patient's medical history without access to an electronic view of their medical record.

3.4 Manner of collection of health information

Health information must not be collected by a health agency:

- a) *by unlawful means; or*
- b) *by means that, in the circumstances of the case:*
 - (i) *are unfair; or*
 - (ii) *intrude to an unreasonable extent upon the personal affairs of the individual concerned.*

It will be demonstrated throughout this report that the intended project scope is within the domains of this rule and subrules. Full auditable consent will be sought from the individual or their representative prior to any access of clinical information by RHED staff.

3.5 Storage and security of health information

A health agency that holds health information must ensure:

- a) *that the information is protected, by such security safeguards as it is reasonable in the circumstances to take, against:*
 - (i) *loss; or*
 - (ii) *access, use, modification, or disclosure, except with the authority of the agency; or*
 - (iii) *other misuse; and*
- b) *if it is necessary for the information to be given to a person in connection with the provision of a service to the health agency, including any storing, processing, or destruction of the information, everything reasonably within the power of the health agency is done to prevent unauthorised use or unauthorised disclosure of the information; and*
- c) *where a document containing health information is not to be kept, the document is disposed of in a manner that preserves the privacy of the individual.*

RGPG policy does not allow for the devolution of security measures, including intra-database measures. However, some measures of security are briefly outlined here ('Users' refers to Pat-Info database Users):

- Physical security
 - The database is centrally stored within a dedicated, secure, server managed by RGPG.
 - Access to the database is restricted to authorised Users only, and their use is monitored.
 - All access tools to the database e.g. passwords are subject to well defined and enforced security measures.
 - Operational information regarding the database and computer systems is restricted to selected authorised personnel.
- Operational security
 - It is part of the employment contract and policies to be read and signed off on during the orientation and on-going employment process that employees/Users must comply with the Health Information Privacy Code 1994 and Privacy Act 1993.
 - It is directed (under the existing Terms of Agreement, RGPG's Information Security and Confidentiality Policy, LDHB's Privacy of Patient Health Information Guidelines Policy, LDHB's Application to view Patient Information Policy, RGPG's Break the Glass Policy, and PrimeWise Individual User) that the information provided will not be used for any other purpose than that which is authorised.
 - These documents form an additional layer of operational and organisational directives to authorised Users to the directives of the Health Information Privacy Code 1994 and the Privacy Act 1993.
 - Further contracts which reflect this Act and information security rules are required to be signed by Users (staff and contractors) when their work involves accessing the Pat-Info database in the 'Individual User' agreement (Appendix 1).
 - It is clearly stated in these documents that access of information on the Pat-Info database is for business purposes only, on a 'must know' basis. No access for personal reasons is authorised or tolerated. Any security breaches will result in disciplinary action.
 - Passwords to access the database are changed at frequent intervals.
 - The Pat-Info database is kept on a secure server managed by RGPG.
 - When authorised Users leave employment their passwords and logins are cancelled immediately.
 - RGPG security and privacy policies and practices are maintained and monitored by the RGPG Privacy Officer.
 - A list of authorised Users is maintained by RGPG.
 - The Pat-Info database has a multi-level access arrangement whereby different levels of access to health information can be enforced depending on the User's level of authority.
 - An auditing system is in place to monitor User use of the Pat-Info database and assist in detecting unauthorised access. Any outputs from this will be available on request.
 - 'Proximity' auditing will occur by default i.e. GP's will receive an automatic notification that the ED interface was accessed for one of their patients. The GP also receives discharge notification from the hospital. A cause for suspicion of inappropriate access would be situations where the GP receives an ED Interface access notification, without this being followed with a discharge notice. As part of the training process, GP's would be instructed about the process they would need to take – i.e. notify the RGPG Privacy Officer.
 - As per Phase 1 of the project, one month after the initial implementation, a full audit, matching the ED Interface access log table with ED discharge notifications, will be completed, followed by random audits.
 - Users found breaching PrimeWise access rules or the Health Information Privacy Code will be disciplined.

- If an LDHB member is found breaching access this issue will be referred to LDHB as an employment issue. RGPG reserves the right to immediately turn that member's access to the Pat-Info database off.
- Users receive training and on-going helpdesk support from RGPG's IT team when authorised to access the Pat-Info database.
- Technical security
 - Appropriate levels of technical security are in place including data back-up, encryption, data and software validation, regular security reviews.
 - In terms of transmission security, the database is hosted on a secure network.
 - Further provision of information regarding technical security is unauthorised by RGPG.

3.6 Access to personal health information

Where a health agency holds health information in such a way that it can readily be retrieved, the individual concerned is entitled:

- a) *to obtain from the agency confirmation that they hold their health information; and*
- b) *to have access to that health information.*

The individual's rights as laid out in Rule 6 of the Health Information Privacy Code 1994 will be upheld without unlawful exception by RGPG and RHED staff and Users.

3.7 Correction of health information

Where a health agency holds health information, the individual concerned is entitled to request correction of the information.

The individual's rights as laid out in Rule 7 of the Health Information Privacy Code 1994 will be upheld without unlawful exception by RGPG and RHED staff and Users.

The health agency responsible for making any corrections, or attaching a statement of correction, is considered to be the source of information collection and retention – the individual general practice, or in some cases RGPG. However, there is a requirement under this Code that the agency to which the request is made is responsible for alerting the appropriate other agency that a request for correction has been made by the individual to information held by that agency.

3.8 Accuracy of health information to be checked before use

A health agency that holds health information must not use that information without taking such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date, complete, relevant, and not misleading.

The purpose of this project is to provide RHED clinical staff with health information details for enrolled patients presenting to RHED, to assist them in their assessment and treatment of the patient.

RGPG and PrimeWise Users have a range of operational and technical measures to ensure that patient information is accurate, complete and up to date e.g. checking with patients when they ring for or present for a primary care appointment, that their address on file is their most current one.

To ensure that RGPG is able to offer RHED the most up to date, accurate and current information available to them, it is proposed under this project that the Pat-Info database will be updated by RGPG daily.

RHED staff accessing a clinical view of patient data will check the accuracy of the information with the individual (or their representative) at an early opportunity, if practicable. To support this practice,

health professionals will be given clear messages in training that the clinical information provided to RHED (sourced from Pat-Info database) should only be used in conjunction with standard history taking methodologies, and should not be relied on by itself. The subset of clinical information may be incomplete (e.g. Information withheld through use of the confidentiality flag).

As an additional layer of protection, warnings on the limitations of the data held in the Pat-Info database will be clearly highlighted on the screen view.

In conjunction with the implementation phase of the project, all participating general practices will be reminded to ensure that data is as accurate as possible, for example, by promptly recording medications prescribed by others and removing those which have been discontinued.

3.9 Retention of health information

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

PrimeWise is a living database – that is, patient information is added and updated on an on-going basis for enrolled patients who are actively engaged in primary care services. In this situation indefinite retention is required for the purposes of providing health services, and the monitoring and management of those health services.

RHED will access a read only data view to obtain the defined subset of information; and this data view source from the Pat-Info database will be updated with more current information every 24 hours.

3.10 Limits on the use of health information

A health agency that holds health information obtained in connection with one purpose must not use that information for any other purpose unless the health agency believes on reasonable grounds that the use of the health information for that other purpose is authorised by the individual concerned.

This project aims to seek further individual auditable consent for the access of the defined subset of data outlined above, at the time that they present to RHED (see section 3.3).

Furthermore, it could be argued that the purpose with which this information will be used under this project is not dissimilar to its original intended purpose (see section 3.1).

3.11 Limits on disclosure of health information

A health agency that holds health information must not disclose the information unless the agency believes, on reasonable grounds that the disclosure is to the individual concerned.

Users will be subject to the RGPG Break the Glass Policy (Appendix 7), which clearly defines the parameters and subsequent auditing/documentation required for instances of emergency access (access without explicit consent) of a patient's health information contained in the Pat-Info database. In brief, all "break the glass" occurrences will be attributed to an authenticated User, time-limited, and audited using the system audit-trail, supplemented by specific information to fully account for the disclosure. This will facilitate a post-event review (if required) of the "break the glass" occurrence.

It is directed (under the existing Terms of Agreement, RGPG's Information Security and Confidentiality Policy, LDHB's Privacy of Patient Health Information Guidelines Policy, LDHB's Application to view Patient Information Policy, and PrimeWise Individual User) that the information provided will not be disclosed to any third party or for any other purpose than that which is authorised.

These documents form an additional layer of operational and organisational directives to authorised Users to the directives of the Health Information Privacy Code 1994 and the Privacy Act 2003.

3.12 Unique identifiers

A health agency must not assign unique identifiers to individuals unless the assignment of that identifier is necessary to enable the health agency to carry out any one or more of its functions efficiently.

This project aims to enable the sharing of individual's unique identifiers in order to enhance the safety and care of enrolled patients on admission to RHED.

The National Health Index number will be used as a unique identifier for patients. Rule 12 permits agencies listed in Schedule 2 of the HIPC, which includes GPs and RHED, to assign NHI numbers, as long as the individual involved is properly identified. In order to assist identification of the patients concerned the project will use the NHI number in conjunction with:

- Patient's full name, DOB and gender
- Street and postal address/s, phone number/s.

4 PRIVACY RISK ASSESSMENT

The Privacy Analysis on the previous pages outlined the scope of the proposed project and scrutinised the components of the project against the criterion and principles of the Health Information Privacy Code 1994 which sits under the umbrella of the Privacy Act 1993.

The following table summarises descriptions of the specific privacy risks identified during the privacy analysis, severity and likelihood of risk, and options to lessen or avoid those risks.

Rule	Project Aspect	Potential risk to or breach of privacy	Risk rating	Options to reduce/remove risk
1	Purpose of collection of health information	No risks to individual privacy were established relating to this aspect. Collection and provision of this health information satisfies several lawful and necessary purposes connected with function and activity for RGPG and LDHB, including care and treatment, administration, and monitoring of the patient and services.	None/Low	
2	Source of health information <ul style="list-style-type: none"> Consent for LDHB to collect the information indirectly from the patient via the Pat-Info database provided by RGPG. 	The information is collected indirectly from the individual concerned in some situations, rather than directly from the individual. The patient has consented however to the collection of the information at the source of collection, the general practice they are enrolled with; and also to the sharing of that information with other health professionals or agencies involved in their care and treatment.	Low	<p>Although technically it could be argued that consent to share the proposed information has already been given through the general practice enrolment process, gaining further explicit consent is seen as a positive benefit.</p> <p>Individuals also have the opportunity to mark health information collected at their general practice as confidential. Any confidentially flagged information will be excluded from access by RHED.</p> <p>Consent for RHED authorised Users to access the identifiable and individual data within the defined subset will therefore be asked in admission procedures when the patient presents to RHED. If consent is denied, the patient's information will not be accessed unless in accordance with provisions set out in the Health Information Privacy Code 1994.</p>

				<p>RGPG has developed a “Break the Glass” policy for when information may be accessed without explicit consent from the patient. This has been endorsed by RAPHs Clinical Leaders.</p> <p>Expressed consent will also be required by RHED from the PrimeWise database owners, Rotorua’s general practices, to view their patient’s information. Every practice will be asked prior to the commencement of this project for consent, and they will reserve the right to opt on or off from this project (Appendix 3).</p>
3	Collection of health information from the individual	No risks were identified additional to those outlined for IPP 2.	None additional	
4	Manner of collection of health information	No risks were identified – collection of health information by the individual’s registered general practice is lawful, fair and necessary.	None	Issues are negated by the consent process outlined above.
5	Storage and security of health information	<p>There are some risks to individual privacy with any project involving the sharing of identifiable individual information.</p> <p>Physical, operational and technical security of the Pat-Info database and the associated data view to be available to RHED staff has been outlined in the preceding section.</p>	Medium	<p>There are multiple measures (e.g. role-based access, 2-factor security and User access auditing) to protect security of the patient information outlined in the preceding section of this document. Please refer to this section for details of security measures which, when in place and operating, should render this risk rating to Low.</p> <p>RGPG maintains very high standards of information security, as can be</p>

				<p>demonstrated through the security levels currently in place to protect the PrimeWise network from unauthorised access by Users and external sources.</p> <p>RGPG reserves the right to complete a Privacy Compliance Audit of Users authorised under this project from within LDHB at any time. Logs of User access will be retained for ten years.</p> <p>These measures should mitigate the risk to Low</p>
6	Access to personal health information	The individual's rights to access their personal health information are not compromised by this project and will be maintained.	None	
7	Correction of health information	The individual's rights to correct their personal information or request attachment of correction to a file are not compromised by this project.	None	
8	Accuracy of health information to be checked before use	<p>This project aims to improve the safety and care of patients on presentation to RHED by enabling clinical staff to view a subset of clinical information jointly agreed by PrimeWise database owners and RHED to be of value in an emergency care setting.</p> <p>There is potential for harm if the RHED clinician accessing the data view does not cross-check the information listed with the patient or their representative i.e. the clinician assumes that the information is complete.</p> <p>The data view can only show what has</p>	Medium/ High	<ul style="list-style-type: none"> ▪ To ensure that information accessed remains the most current and accurate as possible, RGPG proposes to refresh the data view to RHED every 24 hours. The old data view would then be deleted. ▪ A disclaimer warning of the potential for inaccurate or incomplete medical information will be clearly visible on the data view. The purpose being to remind authorised RHED Users that the data view should only be used in

		<p>been entered into the Pat-Info database via the general practice's PMS. The following data quality issues are possible in general practice PMS':</p> <ul style="list-style-type: none"> ▪ Discontinuation of drugs is not always promptly updated; ▪ Missing allergies; ▪ Delay or failure to transcribe into the PMS prescriptions written by others, e.g. Specialist prescriptions, resulting in incomplete medication lists; ▪ Non-compliance with prescribed treatment and use of over the counter drugs is rarely recorded. <p>Clinical information will also be excluded if flagged as confidential.</p>		<p>conjunction with standard history taking methodologies, and should not be relied upon by itself</p> <ul style="list-style-type: none"> ▪ PrimeWise database owners (i.e. Rotorua general practitioners) will be notified and reminded of the importance of keeping patient records as accurate and current as possible (e.g. medication lists) in relation to this specific project. <p>Strict adherence to the processes listed should mitigate the risk to low.</p>
9	Retention of health information	<p>RHED, within this project, must not hold information for longer than which the information may lawfully be used, including holding the information for any purpose to which it is not directly related to the original purpose for which that information was used for.</p>	Medium/ Low	<p>RHED will have no ability to retain or permanently store the information made available to them on the data view outside of entering the data to that particular patient's file. Their view of the data is a fixed, view-only format. These measures should render this risk rating to Low.</p>
10	Limits on the use of health information	<p>Health information being accessed by RHED Users for the purpose of this project should not use that information for any other purpose unless individual consent is obtained or the new purpose is directly linked to the original purpose.</p>	Medium/ Low	<p>It is directed (under the existing Terms of Agreement, RGPG's Information Security and Confidentiality Policy, LDHB's Privacy of Patient Health Information Guidelines Policy, LDHB's Application to view Patient Information Policy, and PrimeWise Individual User) that the information provided will not be used for any other purpose than</p>

				<p>that which is authorised.</p> <p>These documents form an additional layer of operational and organisational directives to authorised Users to the directives of the Health Information Privacy Code 1994 and the Privacy Act 1993.</p>
11	Limits on disclosure of health information	The information obtained should not be disclosed by the Users accessing the data view unless on reasonable grounds or for a lawful and authorised purpose. The information should not be disclosed to any other person unless expressly consented to by the individual.	Low	<p>Refer above to the proposed consent processes during the admission procedure, which should negate some of the risks associated with disclosure.</p> <p>In addition, the documents outlined in Rule 10 also direct that information provided will not be disclosed for any purpose other than that which is authorised.</p>
12	Unique Identifiers	Individual data to be shared in this project include several unique identifiers within the defined subset. These unique identifiers are required to enable RGPG and RHED to carry out their functions (see Rule 1) efficiently and of benefit to the patient. Use of NHI number to identify patients is permitted by Rule 12.	Medium	<p>The risk itself is non-negotiable within this project as the project is based on providing these unique identifiers to RHED Users.</p> <p>The risk of the unique identifiers being misused can be minimised by implementing measures outlined above, with regards to obtaining consent and the multiple security layers to protect the information and the database and data view.</p>

5 PRIVACY ENHANCING RESPONSES / COMPLIANCE MECHANISMS

A number of privacy enhancing responses and compliance mechanisms exist, or can be implemented, to further protect the privacy of individual health information proposed to be shared within the realms of this project. It is recommended that the privacy enhancing responses yet to be implemented be considered, and if accepted, become a priority in order to move this project forward.

Privacy enhancing responses and compliance mechanisms already implemented include:

Measure	Details of Privacy Enhancing Response / Compliance Mechanism	Implemented
Security	<p>Physical security</p> <ul style="list-style-type: none"> ▪ The database is stored on a secure server managed by RGPG. ▪ Access to the database is restricted to authorised Users only, and their use is monitored. ▪ All access tools to the database e.g. passwords are subject to well defined and enforced security measures. ▪ Operational information regarding the database and computer systems is restricted to selected authorised personnel. <p>Operational security</p> <ul style="list-style-type: none"> ▪ It is part of the employment contract and policies to be read and signed off on during the orientation and on-going employment process that employees/Users must comply with the Health Information Privacy Act 1994. ▪ It is directed (under the existing Terms of Agreement, RGPG's Information Security and Confidentiality Policy, LDHB's Privacy of Patient Health Information Guidelines Policy, LDHB's Application to view Patient Information Policy, RGPG's Break the Glass Policy and PrimeWise Individual User) that the information provided will not be used for any other purpose than that which is authorised. ▪ These documents form an additional layer of operational and organisational directives to authorised Users to the directives of the Health Information Privacy Code 1994 and the Privacy Act 1993. ▪ Further contracts which reflect this Act and information security rules are required to be signed by Users (staff and contractors) when their work involves accessing the PrimeWise database in the 'Individual User' agreement (found in the appendices of this report). ▪ It is clearly stated in these documents that access of information on the database is for business purposes only, on a 'must know' basis. No access for personal reasons is authorised or tolerated. ▪ Passwords to access the database are changed at frequent intervals ▪ Each time patient information is accessed, a record is made that 'tags' each view with the User, time, and date that the information was viewed. ▪ The database is kept on a secure server managed by RGPG. ▪ Authorised User login is controlled by 2 factor authentication, using a token and unique Username and password. ▪ When authorised Users leave employment their passwords and logins are cancelled immediately. 	Yes

	<ul style="list-style-type: none"> RGPG security and privacy policies and practices are maintained and monitored by the RGPG Privacy Officer. A list of authorised Users is maintained by RGPG. The database has a multi-level access arrangement whereby different levels of access to health information can be enforced depending on the User's level of authority. An auditing system is in place to monitor User use of the database and assist in detecting unauthorised access. Users found breaching PrimeWise access rules or the Health Information Privacy Act will be disciplined. If an LDHB member is found breaching access this issue will be referred to LDHB as an employment issue. RGPG reserve the right to immediately turn that member's access to the Pat-Info database off. Users receive training and on-going helpdesk support from RGPG's IT team when authorised to access the Pat-Info database. <p>Technical security</p> <ul style="list-style-type: none"> Appropriate levels of technical security are in place including data back-up, encryption, data and software validation, regular security reviews. In terms of transmission security, the database is hosted on a secure network. Further provision of information regarding technical security is unauthorised by RGPG. 	
Policies and Procedures for Privacy Control	<p>Refer above for information on security policies and procedures.</p> <p>A stock-take of policies and procedures for privacy control has been completed for both RGPG and LDHB and found to be sufficient for this project's purposes. Each of the policies/documents listed below complies with both the Privacy Act 1993 and the Health Information Privacy Code 1994, and in most cases states this Act and Code as guiding frames of reference within the policies.</p> <p>Policies reviewed and thought sufficient include:</p> <ul style="list-style-type: none"> RGPG: Health Record Management Policy RGPG: Information Security and Confidentiality Policy RGPG: Data and Information Access Policy RGPG: PrimeWise Individual User Agreement RGPG: Terms of Agreement (established for this project) LDHB: Privacy of Patient Health Information Guidelines LDHB: Application to view Patient Information Procedure LDHB and RGPG Break the Glass Policy <p>The statement that these policies are deemed sufficient does not apply for any these documents altered or new related documents created after this date.</p>	Yes (RGPG) (LDHD)
Technology and system design	<p>There are a range of technological and systemic design measures that are/will be implemented as privacy enhancing responses and compliance mechanisms. Some are listed above within the 'Security' subsection. Others are not appropriate to elaborate on due to organisational intellectual property and confidentiality requirements.</p>	Yes (RGPG)

Review of security risks	<p>This Privacy Impact Assessment was completed by means of assessing the potential privacy and security risks of undertaking this project.</p> <p>RAPHS Clinical Leaders have reviewed and approved the proposed defined subset of data; this approval was gained on 11th September 2012.</p> <p>This document will be circulated as a draft discussion document to the following parties prior to it becoming final:</p> <ul style="list-style-type: none"> ▪ RGPG CEO and Board ▪ RAPHS Clinical Leaders ▪ Existing PrimeWise Users (Rotorua's general practices) ▪ LDHB including, Director for ED, Service Manager for ED (and to others within the LDHB at Service Manager's discretion) <p>This process allows discussion and review prior to the project being committed to further development.</p>	<p>Yes, to be implemented with circulation commencing 11 December 2012</p> <p>(RGPG)</p>
Staff training	<p>All Pat-Info database Users will be provided with training with regards to information protection and security, and privacy and confidentiality considerations, as well as on-going support from the RGPG helpdesk.</p> <p>All RGPG and RHED staff are required to abide by the relevant policies and procedures (as listed above).</p>	<p>Yes</p> <p>(RGPG)</p> <p>(LDHD)</p>
Contingency plans for identifying security breaches to information	<p>There are a range of contingency plans in place and proposed – many of them can be found in the 'Security' section of this table. For example:</p> <ul style="list-style-type: none"> ▪ Each Pat-Info database User's activity will be electronically recorded in a log table which will assist in identifying any access of information that is not appropriate or lawful. ▪ For each access to the data view the patient's registered general practice will receive an automated notification that RHED has accessed their patient's information. ▪ Each User will have a unique login comprising a Username and password, useful in tracking what information Users are accessing. ▪ RGPG reserves the right to conduct a Privacy Compliance Audit of the Users at any time. 	<p>Yes, to be developed for new Users</p> <p>(RGPG)</p>
Steps taken to inform the individuals whose information is being accessed.	<p>Individuals presenting to RHED will be requested for their consent prior to their information being accessed on the data view by RHED administration staff.</p>	<p>Yes, to be developed for new Users</p> <p>(RGPG)</p>

6 CONCLUSION

This Privacy Impact Assessment was completed to comprehensively evaluate the privacy concerns in relation to the expansion of the “**ED Interface with Primary Care**” project to include clinical information.

Phase One of the ED Interface with Primary Care project involved linking RHED staff with patient demographic and general practice enrolment details, with the intention that these staff:

- Have access to up to date address and doctor details and can utilise this in populating patient admission and discharge procedures;
- Can identify locally resident patients who are not enrolled with any general practice, and provide information and support for these patients to be linked into primary care.

The interface went live in June 2011.

Phase Two involves providing a defined subset of clinical information to share at the primary-secondary interface.

Information being provided within the defined subset on the proposed data view includes:

- Problem Lists (diagnoses and allergies)
- Medications (usual medications and acute prescriptions from last 90 days)
- Recent Contacts/Encounters (practice visits) limited to a maximum of the previous 90 days.

The PrimeWise network is used by Rotorua general practices as a central database on which to enter, manage, and store their patients’ demographic, enrolment and clinical information.

This project would offer RHED clinical staff a fixed data view of the subset outlined above. The subset will be exported from the PrimeWise network to a database designed for the purpose of providing this clinical subset view to RHED, called the Pat-Info database. Authorised staff members from RHED will not be able to add, modify, remove or alter data from this database.

Provision of health information by RGPG to RHED serves several lawful purposes connected with the function and activity of both primary and secondary care and treatment of patients. To summarise:

The purpose for enabling the access to a view of clinical information is to enhance patient safety and care in unscheduled consultations when their general practice is closed. Many patients have difficulty remembering all their medications or pronouncing drug names, especially when ill or confused. By accessing primary care clinical records potential benefits include (but are not limited to):

- more efficient assessment;
- reduced drug interaction;
- reduced adverse reactions; and
- reduced duplicate prescribing rates.

This Privacy Impact Assessment has reviewed the project scope and information flows with regards to the 12 Health Information Privacy Rules as stated in the Health Information Privacy Code 1994. Privacy risks identified, and mitigating responses proposed, are summarised in the following table.

This Privacy Impact Assessment will be circulated to appropriate parties within RGPG, PrimeWise Users, and LDHB for a full review and consultative period. Following feedback and amendments, RGPG will establish the technical platform that enables RHED to access a read only data view from the Pat-Info database. These pathways will be tested, before confirming “ready to go live” status to RHED.

The final document will be released and made available as a public document.

Rule	Project Aspect	Potential risk to or breach of privacy	Risk rating	Options to reduce/remove risk
2	Consent for RHED to collect the information indirectly from the patient via the Pat-Info database provided by RGPG.	Clinical information is accessed by RHED without explicit consent by the individual or their representative.	Low	<p>As a default, the patient has already consented to the collection of the information at the source of collection, the general practice they are enrolled with; and also to the sharing of that information with other health professionals or agencies involved in their care and treatment.</p> <p>RHED admission processes will be modified to ensure that all patients (or their representative) on presentation to ED will be asked to give consent for RHED authorised Users to access the identifiable and individual data within the defined subset.</p> <p>Access to information will be based on a role-based permissions framework.</p> <p>If consent is denied, the patient's information will not be accessed unless in accordance with provisions set out in the Health Information Privacy Code 1994 and in accordance of the RGPG Break the Glass Policy in Appendix 7 of this document. All "break the glass" occurrences will be supplemented by specific information to fully account for the disclosure, in addition to the standard audit trail.</p>
5	Storage and security of health information	<p>There are some risks to individual privacy with any project involving the sharing of identifiable individual information.</p> <p>Physical, operational and technical security of the Pat-Info database and the associated data view to be available to RHED staff has been outlined in the preceding section.</p>	Medium	<p>RGPG maintains very high standards of information security, as can be demonstrated through the security levels currently in place to protect the PrimeWise network from unauthorised access by Users and external sources.</p> <p>RGPG reserves the right to complete a Privacy Compliance Audit of Users authorised under this project from within LDHB at any time.</p> <p>These measures should mitigate the risk to Low.</p>
8	Accuracy of health information to be checked before use	The accuracy of individual information accessed by RHED can only be as accurate as the information stored by the general practices on the PrimeWise network.	Medium/High	<p>To ensure that information accessed remains the most current and accurate as possible, RGPG proposes to refresh the data view to RHED every 24 hours.</p> <p>A disclaimer warning of the potential for inaccurate or incomplete medical information will be clearly visible on the data view.</p>

				<p>PrimeWise database owners (i.e. Rotorua general practitioners) will be notified and reminded of the importance of keeping clinical information as accurate and current as possible in relation to this specific project.</p> <p>Strict adherence to the processes listed should mitigate this risk to Low.</p>
9	Retention of health information	This information should not be retained by RHED staff for any other purpose than the stated purpose of this project.	Low	RHED will have a fixed view of the data view only, with no ability to save, modify or remove individual information. This should further reduce the risk of unlawful retention of information.
10	Limits on the use of health information	This information should not be accessed by RHED staff for any other than the stated purpose of this project.	Medium/ Low	<p>A stock-take of RGPG, LDHB, and PrimeWise policies was completed and found to be sufficient for the purposes of this project. These documents form an additional layer to the directives of the Privacy Act 1993 and Health Information Privacy Code 1994.</p> <p>Staff who do not comply with these policies will be banned from the Pat-Info database and referred to their organisation as an employment issue.</p>
11	Limits on disclosure of health information	The information obtained should not be disclosed by any named User accessing the Pat-Info database for any unlawful purpose or released to any person unless expressly consented to by the individual or in accordance to the Privacy Act 1993.	Low	<p>Refer to Rule 2 above regarding the proposed consent process – adding an additional layer of consent to that which is legally required.</p> <p>In addition the documents outlined in Rule 10 also direct that the information will not be disclosed for any other purpose for that which is authorised.</p>
12	Unique Identifiers	The unique identifiers that form the defined data subset of this project are required for RGPG and RHED to carry out their functions efficiently.	Medium	The risk itself is non-negotiable within this project. The risk of <i>misuse</i> of the unique identifiers can be mitigated by implementing the measures outline above, with regards to obtaining consents and the multiple security layers to protect the information and data views.

7 APPENDICES

7.1 RGPG PrimeWise Individual User Agreement



INDIVIDUAL USER AGREEMENT

Please read carefully. Accessing the PrimeWise Patient Information Shared View and its associated data signifies acceptance by the user ("you") of this agreement.

Patient information contained in the PrimeWise Patient Information Shared View, is made available to you to ensure patient safety and continuity of care for those patients presenting to Rotorua Hospital Emergency Department.

The Patient Information Shared View allows clinicians a defined view of the patient's medical record held at participating general practices.

I agree that:

- a. I will use the access for clinical purposes only. No information of any kind will be accessed to satisfy personal curiosity, or for other personal use.
- b. I will not reproduce, distribute or otherwise provide information, to any third party unless the disclosure is in accordance with rule "a" above.
- c. I will keep my password secure i.e. it will not be shared with any other person. In the event that I suspect the confidentiality of my log on credentials have been compromised, I will immediately notify RGPG Support.
- d. I will request the patient's consent to access their records through the Patient Information Shared View.
- e. If the patient is unable to give permission, or access is denied, their information may not be accessed except in situations where the disclosure of the information is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another individual, in accordance with provisions set out in the Health Information Privacy Code 1994 and the RGPG Ltd Break the Glass Policy 2012.


I understand that:

- f. Information that is marked as confidential by the patient's general practitioner will not be visible under any circumstances.
- g. Content from the Patient Information Shared View, is provided on an "as is" basis without warranty of any kind. RGPG cannot guarantee the accuracy or completeness of the clinical information delivered for view from the Patient Information Shared View. Information sourced from the Patient Information Shared View should only be used in conjunction with standard history taking methodologies, and should not be relied upon by itself.
- h. A notification will be sent to the practitioners concerned each time a patient's record is accessed.
- i. Where a patient's record is accessed without their explicit consent, an explanation of the required "emergency" access will be given to the RGPG Privacy Officer and the patient's general practitioner. This will facilitate a post-event review (if deemed necessary, or by patient request).
- j. Use of the Shared View will be electronically recorded in a log table which will assist in identifying any access of information that is not appropriate or lawful.
- k. Where any form of audit has failed to confirm the appropriateness of access:
 - o access to the Patient Information Shared View will be terminated;

Individual User Agreement (page 2)

<ul style="list-style-type: none"> o the privacy breach will be referred to your employer for review and may result in disciplinary action; o the patient will be informed and the matter will be referred to the Privacy Commissioner, the Health and Disability Commissioner, and appropriate professional registration authority. <p>l. Upon request to their general practitioner, a patient will be able to request to see who has viewed their medical record.</p> <p>m. RGPG accepts no liability resulting from misuse of the Patient Information Shared View by users.</p>	
PATIENT INFORMATION SHARED VIEW USER	WITNESS
Name:	Name:
NZMC:	Organisation:
Designation	Designation
Contact Details:	Contact Details:
Signature:	Signature:
Date:	Date:

7.2 RGPG Information Security and Confidentiality Policy

TITLE: Information Security and Confidentiality Policy 	
1. Statement/Purpose/Description	Use of a computer network that is shared by many users imposes many obligations. In particular, data, software and computer capacity have value and must be treated accordingly.
2. Scope	This policy is applicable to all of RGPG Ltd and RAPHs or any member practice staff and employees regardless of their classification as a Health Information Trustee, Health Information Custodian or Health Information User.
3. Definitions	
Health Information Trustee	An organisational unit authorised to create and maintain information and data. The Health Information Trustee, by definition, must have sufficient authority to restrict access to the data within their control.
Health Information Custodian	A Health Information Custodian handles or processes data for the Health Information Trustee. Health Information Custodians could be, but are not limited to, any of the following functional areas: data entry, computer room operators, technical support, courier services, telecommunications, output distribution and systems development and maintenance. In certain cases, a Health Information Trustee may also be a Health Information Custodian.
Health Information User	Anyone who has access to data stored by Information Systems' equipment or facilities. In certain cases, the Health Information User may also be the Health Information Trustee and/or Health Information Custodian.

4. Protocol

All persons will:

- Prevent the accidental or deliberate disclosure of any information pertaining to the health of a patient, via physical or electronic medium, without the express consent of the patient.
- Prevent the accidental or deliberate disclosure of any information pertaining to the financial position of the business, except in accordance with execution of their work responsibilities.
- Prevent the accidental or deliberate disclosure of any information pertaining to the privacy of an employee without the express consent of the employee.
- Prevent deliberate or accidental access to, and use of, any information in physical or electronic files that are stored in the offices or computer systems of RGPG Ltd and RAPHs and member practices by persons not duly authorised.
- Prevent the deliberate or accidental disclosure or exhibition of the contents of any physical or electronic record or report to persons not duly authorised.
- Prevent the deliberate or accidental entry of false, inaccurate, or misleading information into any record or report.
- Prevent the deliberate or accidental removal of any physical record or report, or copies of, from the offices or computer systems where it is stored, except in the performance of their duties.
- Protect their authentication code or device from deliberate or accidental disclosure to anyone.
- Prevent others from accessing or altering information under their assigned digital identity.
- Not utilise anyone else's digital identity to access any other computer systems.
- Be monitored for violations of this policy.
- Prevent the deliberate or accidental use, or duplication of unlicensed software, documents, images or audio tracks.
- Respect the finite capacity of the systems, and thus limit their own use to restrict interference on the activity of other users.
- Report any violation of this code to a Health Information Trustee.

Violators of this code may be subjected to penalties, including disciplinary action, under policies of RGPG Ltd and RAPHs or any member practice and under laws of New Zealand to the extent applicable.

5. Responsibilities and Authorities

5.1 Health Information Trustee:

The Health Information Trustee is ultimately responsible for ensuring the integrity, reliability, accuracy and security of information and data over which they have authority. The Health Information Trustee is responsible for providing the following minimum safeguards:

- Coordinating with systems development and maintenance personnel to ensure that access security controls are implemented to reasonably protect information created and maintained within their area of responsibility.
- Implementing such physical security measures as are appropriate (over terminals, PC's data files, etc) to reasonably ensure the protection of information from unauthorised access.
- Authorising to release or coordinate the release of information to internal and/or external sources.
- Authorising Information Systems development personnel to create and modify application computer programs and systems.

6. Related Documentation

N/A

7. References

N/A

Endorsed by:

Name	Name of Chair	Date
RGPG Ltd and RAPHs Operational Team	Kirsten Stone	30/7/2010

Authorised by:

Name	Chair	Date
RGPG Ltd	Dr Des Epp	17/8/2010

7.3 Participating Practice Agreement



PARTICIPATING PRACTICE AGREEMENT TO Grant access to enrolled patient information for Treatment Providers at

The Practice owners of _____

Give permission for authorised _____ staff
to access and view enrolled patient information extracted from our Practice Management System stored on
the PrimeWise network.

The information requested will be limited to the following:

- Demographic details
- Problem list - diagnoses and allergies
- Medications - usual and acute prescriptions from last 90 days
- Recent Contacts/Encounters¹ (practice visits) – limited to a maximum of the previous 90 days from the date of presentation to RHED².

The subset will be exported from the PrimeWise network to a secure database designed for the purpose of providing this clinical subset view to other health providers. Authorised Users will not be able to add, modify, remove or alter data from this database.

We understand that:

- Patient information may only be viewed after explicit consent has been obtained from the patient or their representative (as defined in the Health Information Code 1994) at the time of presentation to:

- If the patient is unable to give permission, or access is denied, their information may not be accessed except in situations where the disclosure of the information is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another individual, in accordance with provisions set out in the Health Information Privacy Code 1994 and the RGPG Ltd Break the Glass Policy 2012. Any information accessed will be limited to that defined above.
- An automatic notification will be sent to the patient's general practice each time a patient's record is accessed by _____ staff.
- Where the patient's record is accessed without their explicit consent, an explanation of the required "emergency" access will be provided. This will facilitate a post-event review (if required).
- Only authorised clinical personnel who have signed the RGPG Grant of Access agreement will be able to access a patient's clinical information.
- The RGPG Grant of Access Agreement and data views, will contain the following **Terms of Use Disclaimer**:

"Content is provided on an "as is" basis without warranty of any kind. RGPG cannot guarantee the accuracy or completeness of the clinical information delivered for view from the PrimeWise Network. Information sourced from the PrimeWise Network should only be used in conjunction with standard history taking methodologies, and should not be relied upon by itself".

¹ Recent contacts/encounters content will be captured from 1 February 2013, or other mutually agreed 'start' date.

² Information flagged as confidential will not be exported from practice management systems.

Participating Practice Agreement (page 2)

- Use of the database will be electronically recorded in a log table which will assist in identifying any access of information that is not appropriate or lawful.
- Information that is flagged as confidential within our Practice Management System¹, will not be viewable at

TERMINATION

This agreement will continue indefinitely, or until:

- The service is no longer provided to
- Permission is withdrawn by the practice.

Any notification to withdraw permission must be:

- In writing, and addressed to the RGPG Information Systems Manager;
- Signed by a practice owner with tenable practice designated authority.

Access to view enrolled patient information for the practice will be discontinued by the RGPG Information Systems Manager within three working days of receipt of notification.

SIGNED ON BEHALF OF THE PRACTICE OWNERS:

Note: by signing this form the above practice owner has confirmed tenable practice designated authority.

Signed _____

NZMC

Date _____

¹ Please contact RGPG Support for training on how to activate the "confidentiality flag" within your PMS.

7.4 Enrolment form template (correct as at July 2012).

SAMPLE ENROLMENT FORM

PHO Logo

Practice Name
Address
Phone Number

Practice Logo

NHI¹

Title Mr Mrs Ms Miss Dr	First Name ² (Name(s))	Family Name ²	Other Names Known By (e.g. maiden name)	Place and Country of birth ²	Date of Birth ² Day / Month / Year
Preferred Name					
Gender ²	<input type="checkbox"/> Male <input type="checkbox"/> Female				
Physical Address ²	Street or Rural Postcode	Name of Street		Date	
	Suburb			YES / NO	
	City/Town	Postcode		Card Number Expiry Date	
				YES / NO	
Postal Address			High User Health Card ²		Card Number Expiry Date
				YES / NO	
Contact Details	Day Phone	Night Phone	Cell Phone	Email	
Emergency contact	Name of person to contact	Relationship	Phone number	Other contact details	
Which ethnic group do you belong to? ² Mark the space or spaces which apply to you		BLANK FOR PRACTICE TO ADD TO			
New Zealand European					
Maori					
Samoan					
Cook Islands Maori					
Tongan					
Niuean					
Chinese					
Indian					
Other such as DUTCH, JAPANESE, TOKELAUAN. Please state:					

See page 2 - for eligibility, consent and signature

Enrolment in the Practice / Primary Health Organisation (PHO)

I intend to use [practice or doctor name] as my regular and ongoing provider of general practice / GP / First level primary health care services.

I am entitled to enrol because I am residing permanently in New Zealand¹ and meet one of the following eligibility criteria:

a) I am a New Zealand citizen	OR	Yes / No
b) I hold a resident visa or a permanent resident visa (for a residence permit if issued before December 2010)		Yes / No
c) I am an Australian citizen or Australian permanent resident AND able to show I have been in New Zealand or intend to stay in New Zealand for at least 2 consecutive years		Yes / No
d) I have a work visa/permit and can show that I am able to be in New Zealand for at least 2 years (previous permits included)		Yes / No
e) I am an interim visa holder who was eligible immediately before my interim visa started		Yes / No
f) I am a refugee or protected person OR in the process of applying for, or appealing, refugee or protection status, OR a victim or suspected victim of people trafficking		Yes / No
g) I am under 18 years and in the care and control of a parent/legal guardian/adopting parent who meets one criterion in clause a-f above		Yes / No
h) I am 18 or 19 years old and can demonstrate that, on the 15 April 2011, I was the dependant of an eligible work permit holder		Yes / No
i) I am a NZ Aid Programme student studying in NZ and receiving Official Development Assistance funding for their partner or child under 18 years old		Yes / No
j) I am participating in the Ministry of Education Foreign Language Teaching Assistantship scheme		Yes / No
k) I am a Commonwealth Scholarship holder studying in NZ and receiving funding from a New Zealand university under the Commonwealth Scholarship and Fellowship Fund.		Yes / No

I confirm that, if requested, I can provide proof of my eligibility.

My agreement to the enrolment process

NB Parent or caregiver to sign if you are under 16 years

I choose to enrol with this practice as my regular and on going provider of general practice / GP / First level primary health care services.

I understand that by enrolling with this practice I will be enrolled with the Primary Health Organisation (PHO) this practice belongs to, and my name address and other identification details will be included on both the Practice and the PHO Enrolment Register.

I understand that if I visit another provider where I am not enrolled I may be charged a higher fee.

I have been given information about the benefits and implications of enrolment with the PHO, and their contact details.

I have read and I agree with the Health Information Privacy Statement (overleaf).

I agree to inform the practice of any changes in my eligibility.

SIGNATURE²

OR Signed by AUTHORITY²

DATE²

Day / Month / Year

Full Name of Authority	Contact Phone Number	Relationship
Address	Signature of Authority	Day / Month / Year

Detail the basis of authority (e.g. parent of a child under 16):

¹ The definition residing in NZ is that you intend to be resident in New Zealand for at least 180 days in the next 12 months

² An authority is the legal right to sign for another person if for some reason they are unable to consent on their own behalf.

Health Information Privacy Statement	
<p>I understand the following:</p> <p>Access to my health information</p> <p>I have the right to access (and have corrected) my health information under Rules 6 and 7 of the Health Information Privacy Code 1994.</p> <p>Visiting another GP</p> <p>If I visit another GP who is not my regular doctor I will be asked for permission to share information from the visit with my regular doctor or practice.</p> <p>If I am under six years old or have a High User Health Card, or a Community Services Card, and I visit another GP who is not my regular doctor, he/she can make a claim for a subsidy, and the practice I am enrolled in will be informed of the date of that visit. The name of the practice I visited and the reason(s) for the visit will not be disclosed unless I give my consent.</p> <p>Patient Enrolment Information</p> <p>The information I have provided on the Practice Enrolment Form will be:</p> <ul style="list-style-type: none"> held by the practice used by the Ministry of Health to give me a National Health Index (NHI) number, or update any changes sent to the PHO and Ministry of Health to obtain subsidised funding on my behalf used to determine eligibility to receive publicly-funded services. Information may be compared with other government agencies but only when permitted under the Privacy Act. <p>Health Information</p> <p>Members of my health team may:</p> <ul style="list-style-type: none"> add to my health record during any services provided to me and use that information to provide appropriate care share relevant health information to other health professionals who are directly involved in my care <p>Audit</p> <p>In the case of financial audits, my health information may be reviewed by an auditor for checking a financial claim made by the practice, but only according to the terms and conditions of section 22G of the Health Act (or any subsequent applicable Act). I may be contacted by the auditor to check that services have been received. If the audit involves checking on health matters, an appropriately qualified health care practitioner will view the health records.</p> <p>Health Programmes</p> <p>Health data relevant to a programme in which I am enrolled (e.g. Breast Screening, Immunisation, Diabetes) may be sent to the PHO or the external health agency managing this programme.</p> <p>Other Uses of Health Information</p> <p>Health information which will not include my name but may include my National Health Index Identifier (NHI) may be used by health agencies such as the District Health Board, Ministry of Health or PHO for the following purposes, as long as it is not used or published in a way that can identify me:</p> <ul style="list-style-type: none"> health service planning and reporting monitoring service quality, and payment. <p>Research</p> <p>My health information may be used for health research, but only if this has been approved by an Ethics Committee and will not be used or published in a way that can identify me.</p> <p>Except as listed above, I understand that details about my health status or the services I have received will remain confidential within the medical practice unless I give specific consent for this information to be communicated.</p>	<p>Enrolling with General Practice</p> <p>General practice provides comprehensive primary, community-based, and continuing patient-centred health care to patients enrolled with them and others who consult. General practice services include the diagnosis, management and treatment of health conditions, continuity of health care throughout the lifespan, health promotion, prevention, screening, and referral to hospital and specialists.</p> <p>Most general practice providers are affiliated to a PHO. The fund-holding role of PHOs allows an extended range of services to be provided across the collective of providers within a PHO.</p> <p>Enrolling with a Primary Health Organisation (PHO)</p> <p>What is a PHO?</p> <p>Primary Health Organisations are the local structures for delivering and co-ordinating primary health care services. PHOs bring together doctors, nurses and other health professionals (such as Maori health workers, health promoters, dietitians, pharmacists, physiotherapists, mental health workers and midwives) in the community to serve the needs of their enrolled populations.</p> <p>PHOs receive a set amount of funding from the government to ensure the provision of a range of health services, including visits to the doctor. Funding is based on the people enrolled with the PHO and their characteristics (e.g. age and gender). Funding also pays for services that help people stay healthy and services that reach out to groups in the community who are missing out on health services or who have poor health.</p> <p>Benefits of Enrolling</p> <p>Enrolling is free and voluntary. If you choose not to enrol you can still receive health services from a chosen GP / general practice / provider of First Level primary health care services. Advantages of enrolling are that your visits to the doctor will be cheaper and you will have direct access to a range of services linked to the PHO.</p> <p>How do I enrol?</p> <p>To enrol, you need to complete an Enrolment Form at the general practice of your choice. Parents can enrol children under 16 years of age, but children over 16 years need to sign their own form.</p>
<p>Q & A</p> <p>What happens if I go to another General Practice?</p> <p>You can go to another general practice or change to a new general practice at any time. If you are enrolled in a PHO through one general practice and visit another practice as a casual patient you will pay a higher fee for that visit. So if you have more than one general practice you should consider enrolling with the practice you visit most often.</p> <p>What happens if the general practice changes to a new PHO?</p> <p>If the general practice changes to a new PHO the practice will make this information available to you.</p> <p>What happens if I am enrolled in a general practice but don't see them very often?</p> <p>If you have not received services from your general practice in a 3 year period it is likely that the practice will contact you and ask if you wish to remain with the practice. If you are not able to be contacted or do not respond your name will be taken off the Practice and PHO Enrolment Registers. You can re-enrol with the same general practice or another general practice and the affiliated PHO at a later time.</p> <p>How do I know if I'm eligible for publicly funded health and disability services?</p> <p>Talk to the practice staff, call 0800 855 151, or visit http://www.nzohc.govt.nz/eligibility and work through the Guide to Eligibility Criteria.</p>	

Our Health Information Policy

Managing your health information is important to us. The information that you provide assists us in managing your health care.

From time to time we share relevant information about you with other health professionals who are providing or assisting us in providing you with quality care. This is to ensure that you receive the best care.

Information may be compared with other government agencies as permitted under the Privacy Act and also for the purpose of ensuring your eligibility to receive publically-funded services.

Non-identifiable health information may also be used for the purpose of population health research.

Please feel free to ask your Family Doctor or Practice Nurse if you have any questions about how we manage your health information.



This medical centre is a member of

ROTORUA AREA
RAPPS
Primary Health Services

7.6 Sample Information Leaflet for Patients

Information for Patients – Health Information Sharing

If you are enrolled with a Rotorua doctor, other Rotorua health providers e.g. Rotorua Hospital Emergency Department doctors, will be able to access a limited view of your health information, which is held by your usual doctor. **With your permission**, the health professional (e.g. emergency and after hours doctors) will be able to see:

- Medical warnings (a list of your known allergies and adverse reactions to medicines)
- Problem List (a list of your medical conditions)
- Usual medications (a list of medicines that your doctor has prescribed for you)
- Recent medical contacts with your medical centre (e.g. may include information about referrals and recent prescriptions).

Sharing of important medical information helps to ensure that you receive the best possible care from a health professional, even when your usual medical centre is closed. Staff treating you will have a more complete picture of your health and your medical background.

Your permission will always be asked if the health professional wishes to view your health information held by your usual doctor.

If you are unable to give permission (e.g. unconscious), or the doctor believes that your life may be at risk, an emergency or after hours doctor may look at your health information without your permission, in strict accordance with the Privacy Act 1993 and Health Information Privacy Code 1994. This is so they can give you the best possible care.

You can ask your usual doctor to mark certain information as confidential. Anything that has been flagged as confidential will not be visible to other health professionals.

How will I know that my health information is secure?



- Your medical centre stores your health information electronically using the highest standards of security.
- Only health professionals directly involved in your medical care will be allowed to look at your health information.
- Health professionals can only access your health information if they have a password that allows them to look at your health information.
- A record will be kept of everyone who has looked at your health information.
- A doctor who views your information without permission, will be required to fully account for the reasons why they made this access. This may result in a post-event review.
- Your medical centre will be able to check who has looked at your health information if you want them to.

What will happen if I do not want my health information looked at?

- You will receive the same level of care and treatment that you would otherwise receive – although without access to an electronic view of your health information, it may take your treatment provider longer to take your medical history (e.g. checking what medications you are currently taking).

If you have any questions or concerns, please discuss with your usual doctor.

7.7 Break the Glass Policy

 	
<h3>BREAK THE GLASS POLICY</h3>	
<p>1 STATEMENT/PURPOSE/DESCRIPTION</p> <p>“Break the glass” refers to the practice of enabling authenticated Users (e.g. emergency department clinician) access to view a patient’s health information contained in a PrimeWise Patient Information Database¹ under emergency circumstances when that User has not been given explicit consent to view the information from the patient concerned.</p> <p>“Break the glass” relates to an “emergency” and “temporary” authorisation of a User to obtain access to information on a patient that they would otherwise not be permitted to access. This access is temporary and auditable.</p> <p>This policy outlines:</p> <ol style="list-style-type: none"> 1. Scenarios that would trigger a User to “break the glass”; 2. Auditing processes required when the policy is invoked; 3. Consequences for misuse of “break the glass” functionality. 	<p>3 AUDITING</p> <p>The “break the glass” functionality will prompt the User with a warning that he/she does not have access rights required to access the necessary information, that an explanation of the required “emergency” access must be provided, and that the action will be audited. The User may click “Continue” to obtain access to the patient’s information.</p> <p>Each “break the glass” occurrence will be attributed to an authenticated User, time-limited, and audited using the system audit trail, supplemented by specific information to fully account for the disclosure. This will facilitate a post-event review (if required) of the “break the glass” occurrence.</p> <p>An automated alert will be sent to the RGPg Privacy Officer and the patient’s general practitioner (via secure email messaging) to notify all instances of access without consent. A post-event review will be completed by the RGPg Privacy Officer:</p> <ul style="list-style-type: none"> ▪ upon request from the general practitioner (on behalf of their patient); or ▪ in all instances where no explanation is provided for the “break the glass” occurrence. <p>Consequences for misuse of break the glass functionality are outlined below.</p>
<p>2 BREAK THE GLASS SCENARIOS</p>	<p>4 MISUSE OF “BREAK THE GLASS” FUNCTIONALITY</p> <p>An auditing system will be maintained to monitor User use of the Patient Information Database and assist in detecting unauthorised access.</p> <p>All incidents relating to misuse of Break the Glass systems will be referred to and logged by the RGPg Privacy Officer.</p> <p>Breaching of access rules is considered serious misconduct, and Users found to be breaching access rules will be referred to their employer for appropriate disciplinary action by the RGPg Privacy Officer.</p> <p>RGPg reserves the right to turn User’s access to the Patient Information Database off, and will immediately terminate access on notification of suspected misuse.</p> <p>RGPg accepts no liability resulting from misuse of the Patient Information Database by authenticated Users, and this is accepted by Users in the Terms and Conditions of Access.</p>
<p>2.1 A clinical emergency</p> <p>Examples:</p> <ul style="list-style-type: none"> ▪ The patient is unconscious. ▪ The patient presents with an acute injury or illness that is threatening to life or limb and where access to diagnoses or treatment regimens would be beneficial or imperative in supporting treatment decisions made by the User (e.g. emergency department clinician). <p>2.2 In the best interests of the patient</p> <p>Examples:</p> <ul style="list-style-type: none"> ▪ A parent has not consented to their child’s information being viewed and there is a suspicion of abuse (e.g. trauma-related injury). ▪ The patient is unable to give informed consent due to intoxication or other impaired state, such as dementia, and access to additional health information will assist in providing optimal health care. 	
<p>¹ PrimeWise databases are a proprietary service delivered by RGPg Ltd. The information viewable will be limited to:</p> <ul style="list-style-type: none"> ▪ Clinical data sets agreed by Clinical and Organisational Governance as appropriate to each specific database/data view. <p>Nb. Information that has been marked as confidential is withheld from the Patient Information Database.</p>	