Hauraki PHO

Shared Electronic Health Record and Patient Portal

Privacy Impact Assessment

HAURAKI PHO
HAURAKI PRIMARY HEALTH ORGANISATION NETWORK

Matua Rōpu Hauora

Shared Electronic Health Record (SEHR)

Privacy Impact Assessment

This document has been adapted by Hauraki PHO with the kind permission of Compass Health from the BSMC Project Initiative Compass Health

Hauraki PHO acknowledges Compass Health for the sharing of this document

Version: 1.9
Created: March 2010
Last Updated: 30 October 2010
Updated for Hauraki PHO: 30 October 2016
Classification: For General Release

Version Control: Lynne Courtney

Version History

Versio	Date	Change Description	Author Initial
1.2	30 October 2016	Updated for Hauraki PHO	MP
1.3	11 November 2016	Final Review and Editing	MP
1.4	14 November	Review and Editing by Dr Wendy Carroll	WC
1.5	15 November	Edited to include review comments from Geoff King WDHB CIO re CWS access	MP/GK
1.6	11 January 2017	Reviewed by Office of Privacy Commissioner	
1.7	23 February 2017	Review Feedback from OPC HPHO Clinical Workstation Governance Group	
1.8	21 March 2017	Incorporate OPC feedback by Trish Anderson and Monique Pot	MP/TA
1.9	10/4/17	Final review	MP

Contents

1. Introduction

1.1. Overview

In 2011, the New Zealand Health IT Board proposed that by 2014:

- All New Zealanders will have access to their own electronic health information
- All health professionals caring for a person, no matter where they are in the country, will have secure electronic access to that person's full health information[1]

To enable providers to work as patient-centred multi-disciplinary teams, providers need to be able to have access to shared information about patients. The creation of a Shared Electronic Health Record (SEHR) that can be shared through different care settings enables this greatly.

The ManageMyHealth™ (MMH) product, produced by Medtech Limited, offers the ability to aggregate patient information into a summary record accessible by other health professionals without needing a direct connection to each General Practice's medical database. Access is provided through a secure web-browser connection, to authorised users. Patients also have the ability to access their own record via a Patient Portal.

The decision to use the ManageMyHealth™ product by Hauraki Primary Health Organisation (HPHO) was made due to its immediate availability and integration with the majority of patient management systems used within General Practice in the geographical region of the Hauraki PHO region.

This report will assess the potential privacy impact of implementing such a system throughout the Waikato DHB district.

1.2. Report Terms of Reference

This report serves to:

- identify the potential effects an electronic SEHR may have upon individual privacy;
- identify the potential effects using ManageMyHealth™ to provide access to a SEHR may have upon individual privacy;
- examine how any detrimental effects upon privacy might be overcome;
- ensure the project complies with the twelve health information privacy code principles;
- propose mechanisms to mitigate any undesirable impacts identified;
- illustrate to the public that care and diligence has been taken in considering this project and its impacts; and
- inform decision makers about if and in what form the project will proceed.

The scope of the report will cover the initial two phases of the overall project. These specifically deal with:

- the initial setup of the MMH system to receive patient health data from practices within the PHO; and
- the access to the SEHR within specific health care settings.

[1] National Health IT Plan, 2011. An update for 2013/14 has been released

2. Health Records

2.1. Terminology in Health Records

It is important for the reader to understand the basic terminology of electronic medical records used in this document and project. There are various subtly different terms used to describe electronic patient health records. Each term when used deliberately describes different scenarios and solutions.

2.1.1 Electronic Health Records

The Electronic Health Record refers to a full health record for a patient that is held in electronic form by a third party, and can be amended in real-time by appropriate health professionals and carers. This term is used internationally and is generally well understood by health informaticians. It is sometimes used interchangeably with the terms Electronic Patient Record and Electronic Medical Record.

This record typically would be the sole health record for the patient. Health Professionals treating a patient would use the record directly, with no need for any ancillary notes or records. It represents a complete and detailed longitudinal medical record for the patient in all care settings in which they receive health care.

While an Electronic Health Record allows all health professionals involved in patient care to work from the same set of information, this project does not intend to attempt to create such a record.

2.1.2 Shared Electronic Health Records

A Shared Electronic Health Record (SEHR) is what this project is proposing to create and provide to health professionals and patients. The New Zealand Health Strategy highlights the importance of digital solutions to support a smart health system. The Ministry is working on an indicative business case for an electronic health record, which will be focused on providing better access to health information for patients, clinicians and health system planners. The indicative business case is expected to be completed by mid-2017 http://www.health.govt.nz/our-work/ehealth/digital-health-2020/electronic-health-record [2].

A SEHR refers to a summary record of health care information. It contains only significant summary and basic demographic information. Internationally, the term Summary Care Record is used to describe such a record. In New Zealand, the use of the term “Shared” rather than “Summary” has been coined most recently by the National Health IT Board in their Draft National Health IT Plan. This document will use the emerging New Zealand terminology.

A SEHR can be used by health professionals to share information about patients and their treatments. Typically, the SEHR would be sourced from a complete medical record held by each specific health professional treating the patient. A health professional would use their own system for detailed information on the patient’s history and treatment information.

2.1.3 Personal Health Records

A personal health record is a collection of a patient’s health information held and set-up by the patient themselves. In its most basic form, this can be done in a paper-based mechanism. Within the last few years, large computing providers, such as Google and Microsoft have provided tools that enable health consumers to set-up their own electronic record.

Most notably in New Zealand, a company called Doctor Global had started providing electronic Personal Health Records to patients almost a decade ago.

[2] http://www.health.govt.nz/our-work/ehealth/digital-health-2020/electronic-health-record

A Personal Health record is separate and distinct from the SEHR. MMH provides an interface to both of these types of records. The Personal Health Record on MMH is referred to as the Patient Portal. This project is mainly focused on the aspects of MMH that can be used for the SEHR.

2.2. Rationale

Sharing of patient information between health professionals already occurs. The three most common scenarios of this between care settings are:

- either through a referral process, usually including a form detailing relevant or pertinent information;
- through discharge summaries that are supplied when patients are discharged from services; or
- verbally through one clinician making contact with another to discuss particular aspects of a patient's case.

At times, verbal transfer is used in conjunction with either of the other two – often as a result of the treating health professional's need to clarify aspects of information contained on a referral form or discharge summary.

Obtaining patient information verbally from general practitioners, usually over the phone can also be difficult for other health professionals. Often, primary health care professionals are not available at the times other health professionals working within acute and emergency settings need to speak to them, as they tend to work during extended business hours and patients present to EDs 24 hours a day, 7 days a week.

When unplanned presentations to health services outside of general practice do occur, patients can often recount important or recent medical history. This method of information collection is valuable in all care settings. It can be couched in lay-terminology or not be specific enough to be entirely useful to treating health professionals. This is particularly true where patients are disoriented or unable to communicate clearly.

In situations where patients are referred to outpatients and for planned admissions, they continue to be managed in general practice until they are seen. Delays in seeing patients in these settings are common. This leads to the information that may accompany the patient at the time of referral being potentially out of date as management in general practice has progressed with the patient over time through the ordering of lab test and treatment trials.

All of these situations lead to inefficiencies in the use of health professionals' time, information that is less detailed than it could be and ultimately delays for patients in triage or treatment. Health professionals presently do very well with the limited information they are able to collect. This project aims to help them gain more complete information on a patient's medical history in these situations.

2.3. Information Flows

There are three main flows of information within this project:

- General Practice to ManageMyHealth™;
- ManageMyHealth™ to Care Settings Outside General Practice; and
- ManageMyHealth™ to Patient.

2.3.1 General Practice to ManageMyHealth

The first stage of this information flow involves communicating with General Practices who are members of Hauraki PHO to advise them of the project and seek agreement to take part.

A communications plan will be executed, to inform health professionals and patients of the intention to include all Hauraki PHO registered patients in the SEHR project. This communication will also outline their ability to opt-out of this process.

Patients have the right to opt off the SEHR. Patients are requested to make contact with their General Practice (GP or Practice Nurse) to discuss the SEHR. If following discussion, the patient still wishes to opt off the SEHR, the patient and practice is requested to complete an opt off form for administrative purposes, which the Practice will then scan and email through to the Hauraki PHO SEHR Administrator. The SEHR Administrator will then add the patient's details to an Opt off Register and then log on to the SEHR and select Opt off for this Patient. The PHO will be responsible for maintaining the list of patients who wish to opt-out of the project.

The 2nd stage is a subset of the Patients Historic Health Information is transferred on a set date from the general practice patient management system via a SEHR internet connection (SSL) to the MMH server. The level and mechanism of security for information transfer is similar to that used in the banking industry for internet banking.

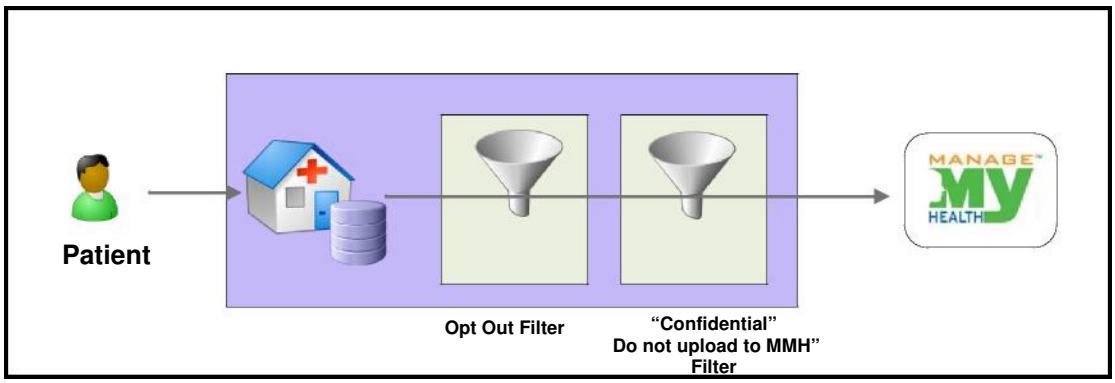

Figure 2: SEHR Maintenance

The third stage of this information flow is the maintenance phase, where new information is added to the SEHR. This is usually done when the patient presents to their General Practice, or when new information is added to the patients record as a result of a recent presentation (such as new lab result information being returned from the laboratory). Only information that has not been marked as "confidential" or "Do Not Upload to MMH" for patients who have an existing SEHR or Patient Portal record is sent to MMH.

Patients wishing to gain access to their own Patient Portal via MMH will be required to visit their General Practice and to have a valid and accessible email address. They will need to meet face-to-face with one of the general practice team in order to access their own health record on the Patient Portal. Patients will then be required to activate their patient portal account and enter a password. If they lose their password at a later date, they are able to have it reset and have a new password sent to their nominated email address.

2.3.2 ManageMyHealth™ to Alternative Care Settings

When a patient presents to a care setting in which MMH is available, such as the Emergency Department or After Hours, the treating health professional should establish verbal consent from the patient to view their SEHR and document this in the patient's record. Evidence shows that even with widespread and targeted publicity about SEHRs, the majority of patients don't recall such publicity at a later date [9].Obtaining such consent has been noted as one of the success factors in Scotland's Emergency Care

Summary [10] and further safeguards against any patient who is unaware that their SEHR is accessible in the particular care setting in which they are presenting.

Once consent to view the record is established, the health professional will need to determine the patient's demographic details such as name and address and National Health Index (NHI). In most care settings, this step would be routinely done in order to appropriately associate health care information with the individual. Locating the patient's NHI can usually be done by using the patient's name and date of birth.

Once patient's details are confirmed they will then be able to log in to MMH and look at the patient's SEHR, if it exists.

The most basic form of sharing of patient information is through a SEHR web browser session (shown in Figure 3: SEHR Sharing in a Hospital via a Web Browser). The internet security settings and other security requirements are discussed in section 3.1.5 of this document.

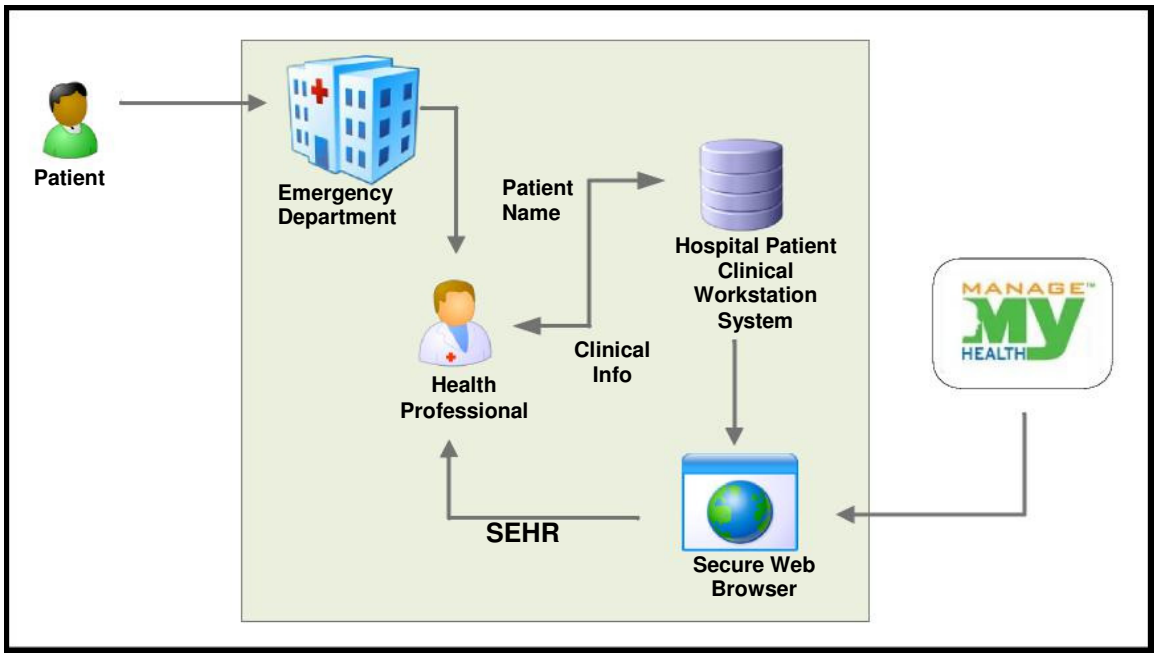

Figure 3: SEHR Sharing in a Hospital via a Web Browser

Figure 4 shows access to the SEHR via the Hospital Patient Clinical Workstation (CWS). In this case the CWS has a direct In Patient Context interface to MMH. What this means is that the DHB Clinician does not search within MMH to find a patient record, they view the MMH record for the specific patient that the clinician is accessing through CWS. The health professional log in to (using a unique & secure username & password) CWS, and their access to the patient record within both CWS and the SEHR is recorded and audited. Such an arrangement in this care setting reduces the complexity to health professionals needing to navigate scores of systems all containing patient information. In this situation, the health professional does not need to undertake a two-step process of identifying the patient's NHI separately to looking at their record. Access to the CWS, as well as access to MMH is logged and audited by the hospital and SEHR project respectively.

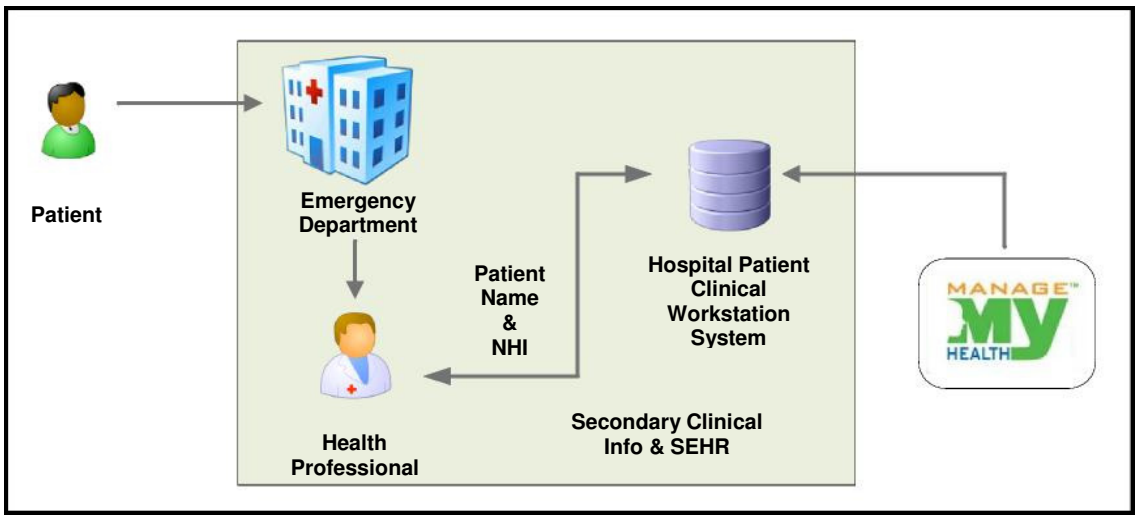

Figure 4: SEHR Sharing in Hospital with Systems Integration

The care settings where the SEHR may be made available will include:

- General Practice;
- Hospital Emergency Departments;
- Hospital Outpatient Departments;
- General Hospital Departments;
- After Hours Medical Centre's;
- Hospice
- Paramedic and Ambulance Services;
- Elderly Care Facilities; and
- Community Pharmacies.

The summary information available to providers in these care settings will include:

- medical classifications in the form of Read Codes;
- consultation notes - free text of clinically subjective or objective daily records (from the date of initial data upload)
- prescribed medications;
- inbox records i.e. lab and x-ray results;
- medical warnings (allergies, contained within PMS);
- immunisations; and
- recalls.

Different views of information will be available in different care settings. For example, within an Emergency Department, all the summary information listed above would be available. Within other care settings, such as community pharmacy, only prescribed medications and allergies may be available.

Where other Health Organisations request to have access to the SEHR, a formal request will be required to be made to the HPHO Clinical Workstation Governance Group. The group will consider the request and

if accepted will decide on which sections of the patient's health information will be made available. General Practices will be provided with communication for each accepted request.

2.3.3 ManageMyHealth™ to Patient

A Patient is able to have access to their own Personal Health Record via the MMH Patient Portal. Patients will need to attend their general practice to register and receive their login information.

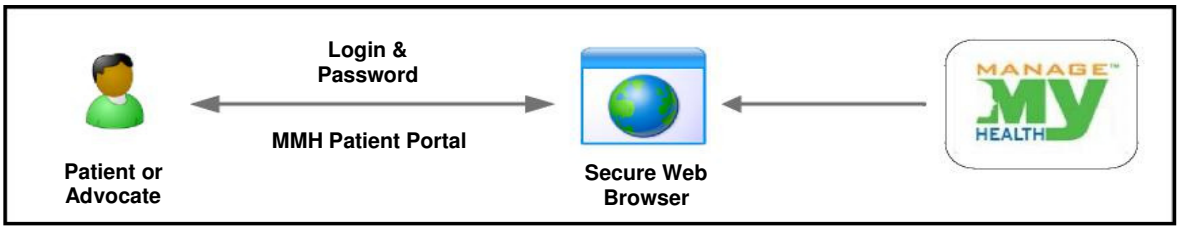

Figure 5: SEHR Patient Portal Access By Patients

2.3.4 Access Query and Audit

HPHO will facilitate an audit process investigation which will consist of reviewing the patient's SEHR access record, having appropriate health professional peers investigate any clinical context associated with the accessing of the patient record including obtaining background information directly from health professionals. This process will be run in conjunction with existing clinical governance such as already established Clinical Boards. Where the patient requests it, a summary of findings, explanations and any educational material will be provided to the patient addressing their concern or request. Any non-clinical staff completing an audit process will be unable to access any clinical information. As such, having an auditing process for these auditors would be unnecessary. All clinical staff, even in the course of conducting an audit, would be subject to the same audit process. Patients who have access to their own Personal Health Record, via the Patient Portal will have the ability to review the access history of the SEHR by others.

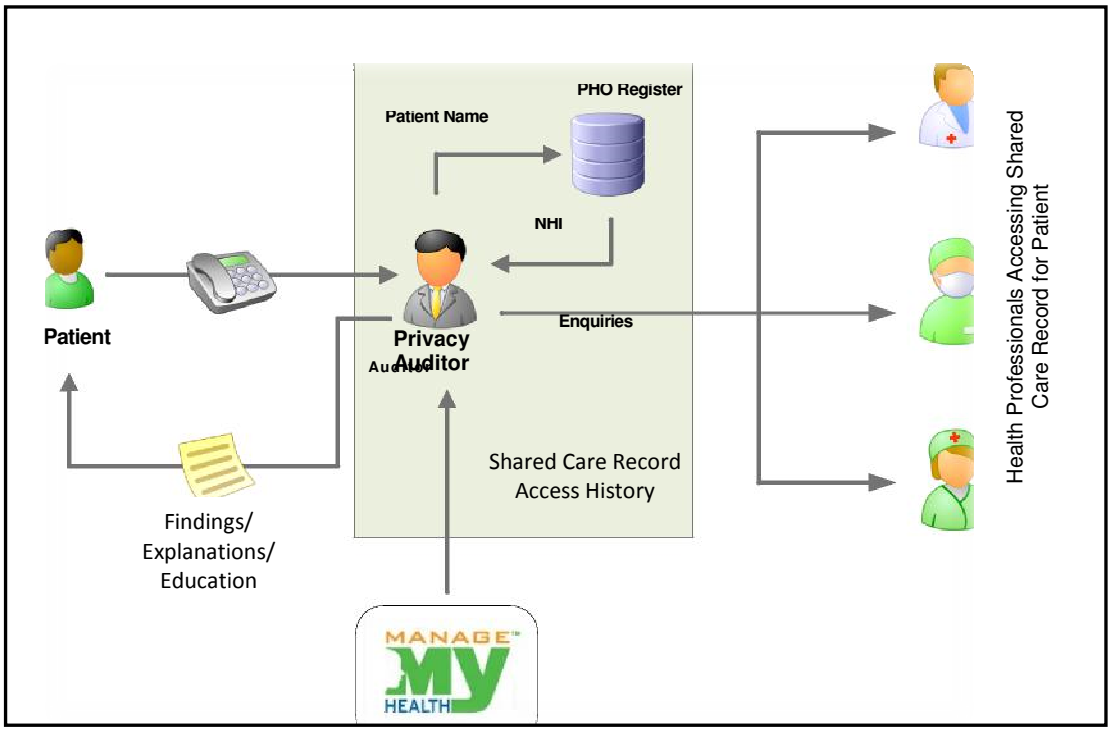

Figure 6: SEHR Access Query Audit Process

3. Privacy Impact and Analysis

3.1. Privacy Principles Considerations

3.1.1 Rule 1: Purpose of Collection

Rule Rule 1 of the Health Information Privacy Code (HIPC) requires that information be collected only for a lawful purpose that is related to the function or activity of the health agency.

Current Currently, health professionals record information on patients' medical history and treatments. They do so primarily to provide a record of their medical care and information pertinent to the decisions made in doing so. This record has uses in the ongoing treatment of the patient, as well as providing a basis for any future medico-legal need. They also record the information for the purposes of sharing relevant information with other health professionals at the time of referral to other services to ensure a reasonable standard of continuity of care to the patient. In some situations the information is recorded for statutory and or statistical purposes.

Impact In terms of collection of information, this project does not change any of the existing purposes of collecting the information. It will have no impact on the purpose for which information is collected from a patient.

3.1.2 Rule 2: Collection from Source

Rule Rule 2 of the HIPC addresses the need for health information to be collected as directly from the source of the information as possible. In most cases, this is directly from the individual or as a direct result of the individual consenting to clinical tests.

Current In almost all instances in General Practice at present, information is collected directly from the patient. This is usually done with the health professionals and the patient in either a face-to-face, or telephone setting or from email from a Patient Portal. There are exceptions as to when the information can be collected from someone other than the patient and these exceptions are provided for in Rule 2 of the HIPC as, in some situations, information is sourced from parents, guardians or caregivers.

Impact This project does not change the source of the collected information. The patient still presents to their health professional who collects the information in the same way as before. Other health professionals accessing the SEHR would then be viewing information entered by the health professional responsible for the collection of it directly from the patient themselves.

3.1.3 Rule 3: Collection from Individual

Rule Rule 3 addresses the need for those collecting the information to ensure that the individual is aware of the information flows and the purpose of those flows. Its intention is to provide autonomy to the individual in the control of their health information [11]. Rule 3 ensures awareness by the patient of what is happening with their health information. The following sub-rules are particularly relevant to this project:

- who the intended recipients of the information are (3-1-c)
- the agency that will hold the information (3-1-d-ii)
- whether or not the supply of information is voluntary or mandatory (3-1-e)

- the consequences for that individual if all or any part of the requested information is not provided (3-1-f)
- the rights to access to, and correction of health information provided by rules 6 and 7 (3-1-g)

The HIPC indicates that although sharing information with other pertinent health agencies involved with the patient's care is good practice, it should only be done with the individual's knowledge[11]. This rule is intended to assist the awareness of patients to what is happening with their health information, not to require consent from them for it to happen.

Current Currently, the agency that holds the health information for patients is the patients' general practice. This is often done on the same site as the practice itself. In some instances, practices sub-contract other providers to maintain their computer systems. In these instances, the sub-contractor is acting as an agent for the practice itself. There will be contractual agreements in place that ensure the sub-contractor adheres to the rules under the HIPC. This will be the responsibility of the General Practice.

The supply of most information to a provider in the care setting in general practice is voluntary. Patients can choose to disclose particular details if they wish.

Patients are made aware that they have the right to access their health information through brochures and posters displayed in general practices.

Impact This situation changes slightly with the introduction of this project. The primary storage of the patient's medical information remains within the general practice itself. This information, in summary form, is then transferred to a third party organisation responsible for storing and providing appropriate authorised access to that information. This third party organisation may also sub-contract its services for storage to another agency. The HIPC[11] outlines on page 22 that the need to make the patient aware of the details of who is holding the information is so that "they can exercise their rights of access" to it.

The need to know who is holding the information, for the purposes of accessing the information is for all intents and purposes the general practice still. The information being held by the other parties are only acting as agents for the practices and, as such, only hold a copy of the information that the practice generates. It will still remain the responsibility of each organisation to maintain contracts with their sub-contractors to ensure the subcontractors adhere to HIPC rules.

The supply of any information by the patient to the General Practice is voluntary. This project changes the decision-making process that a patient and their health professional must make with regard to the information that is shared. Presuming the patient decides to disclose information to their general practitioner, they must also decide whether they wish to have that information disclosed to other health professionals by having it included in their SEHR.

This places an additional burden upon the health professionals counselling patients. They must make the patient aware of the consequences of including or withholding information from their SEHR.

The consequence of not supplying information within one's SEHR is relative to an improved level of care others will experience. This project aims to improve the level of patient care within care settings outside general practice. It does this by allowing health professional's access to a patient's SEHR.

Where practical, consent should be obtained from the patient by the health professional before accessing the patient's record on the SEHR.

Health professionals are obligated to disclose some information for some conditions or situations, usually to national registries. This mandatory disclosure to these registries does not change. The patient, although not having the choice whether this information goes to such registries, would still have the choice to have the same information excluded from their SEHR. Mandatory disclosure does not affect a patient's ability to control what goes into their SEHR. In such circumstances, the health professional will still counsel the patient as to the possible consequences of their decision to not include such information within their SEHR.

Posters and brochures will continue to be produced with updated information to help inform patients on what happens with their health information and their rights within that.

In order to address and mitigate some of these changes and the impacts that they may potentially have on the patient, it is advisable that four things are done as part of the project:

- a public communication plan is executed which will include notification in local and community newspapers
- practices will be supplied with posters of the notification outlined above and will be required to display these posters in a prominent position within their practice;
- practices are supplied with patient information brochures, practice would be required to make these available to patients wanting them within their practice; and
- a provider communication plan is executed, including provider meetings and training

3.1.4 Rule 4: Manner of Collection

Rule Rule 4 addresses the need to ensure that information is collected in a fair manner.

Current Health Professionals have clinical and business processes for collecting information on patients during the course of their interactions. These processes differ depending on the type of each health professional (doctor, nurse, counsellor etc.). These processes are already governed by professional quality standards and appropriate statutory registration bodies and professional groups. However, it is important to note that this rule is not just limited to the collection of information directly from a patient, and includes information collected from a parent or from another health professional.

Impact The collection of information for this project does not differ from the collection of information in the course of normal clinical practice within general practice.

3.1.5 Rule 5: Storage and Security

Rule Rule 5 addresses the need for agencies holding the health information to secure it appropriately. No absolute measures are outlined, as the appropriate level of security depends on the sensitivity of the information.

Current A patient's medical history is stored within the general practice systems. Appropriate safe guards to prevent against physical, operational, technical and communication threats already exist. The Health Information Security Framework Essentials and Recommendations [12] is an appropriate document for practices, PHOs and other health agencies storing health information to consider and implement where appropriate.

Almost all general practices are connected to the internet, usually by a broadband internet connection. This internet connection is used primarily for the use of normal business email, web browsing and for creating secure messaging gateways to communicate electronically with other health professionals (most often using the HealthLink product).

The terminology “surface area” is often used to describe how much potential there is for threats to attack the security of a system. Having an internet connection is a genuine security risk. The associated surface area for attack it provides is extremely minimal if it is configured correctly. Having an internet connection has a high business benefit which outweighs the associated risks.

Impact This project increases the surface area of the systems that hold patient’s health information. The aggregated record is stored in a manner that is accessible over the internet. It will be secured with a single-factor authentication mechanism, requiring anyone wishing to access it to have a matching pair of username and password. The risk of interception of data is low with the use of securely encrypted web browser connections. The risk of an unauthorised user guessing a provider username and password combination is again low, as long as passwords that are used are kept secret and relatively strong. All reasonable safeguards will be taken in relation to this project.

The risk with the most likelihood of occurring is one where a patient or provider compromises the system security by inadvertently or deliberately giving others their username and password. To mitigate this, it will be important within the patient information to stress the importance of keeping their username and password safe and to only give it to other people that are acting as their guardian or advocate if they wish to. It will also be important to ensure that health professionals are educated fully as to their responsibilities and measures that they need to take to ensure the safety of the system.

Organisations with staff accessing the MMH system will be required to ensure that the employment agreements that they have with their staff have appropriate privacy clauses. These will include statements that actions associated with compromising network security or patient privacy are considered serious misconduct. Organisations will also be asked to ensure that their network, processes and procedures meet a minimum security standard (based on HISO’s recommendations [12]).

Where staff has been found to have carried out serious misconduct, the most likely outcome within New Zealand organisations is the dismissal of that staff member. A finding of serious misconduct due to a breach of privacy would also likely result in the incident being reported to the appropriate professional body, including the Office of the Privacy Commissioner This may also result in further sanctions upon that individual extending beyond their current employer. Such a deterrent should be sufficient to dissuade the majority of staff to not engage in behaviour that could lead to this.

A SEHR Administrator from HPHO will be appointed and will facilitate audits of access to the system. Every time a health professional views a patient record, access to that patient record is logged on the MMH audit trail. An audit will also be done at random on a sample of health professionals and patients. In undertaking audits, the SEHR Administrator will have access to clinical information and will be assessing patterns of access only. Where further investigation of irregular access is required, such investigation will be carried out by fellow health professionals. This mechanism is not intended to act as a front-line mechanism to prevent unauthorised access, but rather act as a monitoring and deterrent mechanism. As such, it will be important to remind providers from time to time that their access to the system is being audited.

The Clinical Workstation Governance Group will ensure that there is suitable policy and procedures established to deal with privacy investigations, requests and breaches.

Patients who choose to access their own personal health record through the portal will also have the ability to audit who has accessed their record by logging on to their own Patient

Portal account. Patients will also be able to contact the SEHR Administrator or their General Practice team to request information as to whom has accessed their record on the SEHR.

3.1.6 Rule 6: Access

Rule

Rule 6 pertains to a patient's right to access their own health information, and the need to inform patients of their rights under Rule 7.

Rule 6-2 sets out the requirement of the patient to be informed that they are entitled to request the correction of information held on them.

Rule 6-1-b pertains to a patient's right to know whether an agency holds information on them.

Rule 6-3-a also sets out the right for health professionals to refuse a request for access to a patient's health information. The Privacy Act sets out in sections 27 – 29 a number of reasons why access to a patient's personal health information could be refused to him or her. As such, this scenario needs to be considered.

Current

There is no unified health record in New Zealand at present. If patients wish to view their health information, they must make contact with the appropriate heath care organisation. In the case of accessing their health information held in General Practice, they need to make contact with the appropriate general practice. They may need to book an appointment with their health professional, or request a print-out of the electronic information that is held for them.

Such requests usually require a person-to-person interaction, at which time, the patient can be advised that they are entitled to request that information be corrected – which must be done according to sub-rule 6-2[11].

General practices remain the stewards of patient health information in the current situation.

Under certain circumstances, health professionals are entitled to withhold information from a patient after an official request from the patient for it, subject to the withholding grounds in Section 27-29 of the Privacy Act. Where they wish to do this, they make this judgment after the patient makes the request for information. They have twenty working days after the receipt of the request to make this determination. General Practice has existing processes to deal with this situation.

Impact

Patients will be able to access their own summary health information held within their Patient Portal account directly, once they have gone through appropriate identity verification checks and are issued with a username and password for MMH. They will also need access to a "computer" or other device and the internet.

The existing mechanism of requesting information directly from the appropriate general practice will still be available. This may be preferred by those patients that don't have access to a computer or the internet, or do not wish to obtain a username and password for their record or for those that wish to obtain more detail on the medical information held on them.

Sub rule 6-2 says that the individual, when given access to health information, must be advised of their right to correct that information. There remains a requirement to have a face-to-face meeting in order for a patient to obtain a login to MMH. This would be the most appropriate time to ensure that the patient is advised of their rights in this regard.

Clearly, when a patient is first given their username and password for MMH so that they may access their own Personal Health record, they should be advised of their rights to correct information. This should be built into the practice or PHO level process of providing access to MMH.

For a health professional to withhold information from a patient, the health professional must make this judgment at the time information is entered into their patient management system or prior to the patient requesting a username and password for MMH to their own record. Although there is limited ability to retrospectively flag items of information as "confidential" or "Do Not Upload to MMH" and have this removed from the SEHR, there is no easy way for a health professional to know whether the patient has already sighted that piece of information.

If a provider wishes to make only a portion of a patient's record unavailable to them, they can do so by marking the relevant pieces of information "confidential" or "Do Not Upload to MMH" within the Medtech32 and Medtech Evolution systems. However, by marking the record as "confidential" this also makes this information unavailable to other health professionals.

If the provider has determined to only make some of a patient's health record available, the patient may still request that the information withheld is disclosed.

Rule 6-1-b pertains to a patient's right to know whether an agency holds information on them. The SEHR Administrator will have the ability to field such requests within the limited scope of confirming or not whether the MMH patient portal has information on that individual. Any non-clinical staff that undertakes this function should explicitly be prohibited from viewing any clinical information as part of this process. They only need to be able to see enough non-clinical information to accurately establish whether a record for any individual exists. In line with procedures in place, patients will also be able to access their personal health information by being given a username and password to the Patient Portal. If the patient wishes to make a request to have information corrected, they will still be able to do so directly with their general practice or by contacting the PHO.

3.1.7 Rule 7: Correction of Information

Rule Rule 7 outlines the patient's entitlement to request the correction of information held on them. It also outlines an agency's obligation to correct information when it is wrong.

Where an agency receives a request to correct information but they do not wish to correct the information, the agency is obligated under rule 7-3 to attach a note to the patient record outlining the request and subsequent refusal.

Current Normally within general practice, this would be done within the daily record, or as an attached note to a particular data item. The patient would, after requesting and sighting their medical information make a request to the general practice to have an item of information corrected.

The practice might arrange an appointment with the patient and the health professional responsible for the information. The Health Professional must either make a correction in the patient's record or if the information was accurate, make a statement in the patient's record in the PMS advising as to the patient's request, why the information was not corrected and grounds to not change the information. It should also be recorded that the patient was advised of their right to make a complaint to the Privacy Commissioner about the decision.

Impact As per Rule 6, facilitating better access will empower the patient to ensure that their information is correct and accurate and gives them the ability to review that any correction has occurred.

Correction of the record directly within MMH itself is not possible. The system is an aggregator of information, rather than an information repository in its own right. Correction will be sought at the source general practice in these cases.

The MMH Operational Team will be responsible for directing patients to their general practices to get the information corrected.

This project will include the upload of patient consultation notes as part of the SEHR. Particular data items within Medtech32 and Medtech Evolution such as classifications allow the inclusion of "notes", which are included with the SEHR data. Providers will be educated to ensure that they record any disputes to the accuracy of information within the "notes" section of these data items. The classifications data, which may contain diagnosis information that is a result of opinion rather than fact, is the most likely data that would have requests for correction and refusal. Most other data items, such as prescribed medications, lab results, immunisations, recalls and allergies are medical facts and are clearly either accurate or inaccurate.

3.1.8 Rule 8: Accuracy

Rule Rule 8 requires information to be accurate to a level commensurate with that for which it is being used.

Current At present, providers need to record information in patient's health records in an accurate and precise manner to ensure that they meet their duty of care. They need to also do so to ensure from a medico-legal standpoint there is sufficient information to document and justify their clinical decisions. They already share this information with their colleagues that work within the same general practice when they are on leave and other health professionals must see their patients. They also share parts of this information with other health professionals outside of their general practice when they refer the patient to other health services.

When referring the patient to other services, the health professional in general practice is able to contextualise the information they share, or when necessary elaborate. This is done at the time the referral information is prepared.

Impact This project intends to make summary information and free text of clinically subjective or objective daily records available to health professionals working outside of the general practice setting. The summary information available is categorised information.

Providers use the categorisation systems within the PMS in slightly different ways. This introduces some issues of data quality. Usually within General Practice, context can be provided within the clinical notes. Each of the categorisation items can however have notes attached to them. These notes are intended for short pieces of information that are associated with that particular item (i.e. a diagnostic code).

Along with the duty of care of the health professional in general practice to record information, there is also an onus on the duty of care of the health professional using the information in other care settings. It is important that health professionals using the SEHR understand its limitations.

The intent of the summary medical record is not for it to be used in isolation, but in conjunction with existing practices around information collection, including a full history and physical examination. The SEHR should always be considered an adjunct to good clinical history-taking, and used to clarify or to prompt for additional information from the patient. Providers need to be given this message clearly, and this will be included prominently in all provider training and education around using the SEHR.

Patients may often recall non-specific or imprecise details about their recent medical care for instance. The SEHR would enable providers to clarify the specific details of conditions or medications that patient may refer to. It may also prompt the current health professional to ask the patient additional questions about parts of their medical history that they have omitted where the health professional believes it may be relevant.

3.1.9 Rule 9: Retention

Rule Rule 9 states that a health agency must not hold health information longer than is required for the purposes for which it may be used. The purpose of the information being collected in the SEHR is to provide other health professionals outside the patient's general practice setting with relevant medical history.

The Health (Retention of Health Information) Regulations 1996, states that health information should be retained for a minimum period of ten years from the last attendance. It does not stipulate a maximum period.

Current With electronic records, a general practice would hold a copy of a patient's record indefinitely, even once they are deceased (the patient record would be marked as such, but it would not be deleted or removed from the system). Even in the case of a patient transferring General Practices, the incumbent practice would continue to hold a copy of the medical records, even when those records are "transferred" to the patient's new practice.

Impact There are potentially four situations in which the retention of information within MMH must be considered. They are if the patient:

- dies;
- chooses to no longer have an SEHR;
- moves general practices within the District; and
- moves general practices outside the District.

For the purposes of this project, MMH is being used to deliver a SEHR. MMH also has a component that provides for a Personal Health Record for the patient, which allows the patient to record their own information about their health. This impact assessment addresses the use of MMH to deliver and store the SEHR information only. The aspect of the patient's record that pertains to their Personal Health Record should be covered under existing MMH privacy assessments and statements.

The aggregated record is a reflection of the information stored within general practice and, as such, in its present form, would hold patient records indefinitely also. This situation may not be desirable from a privacy standpoint, as the purpose of the aggregated record is to provide medical care to the patient (rather than a record of their treatment for legal or medico-legal reasons – which may be a justification as to why a general practice would retain medical records long past a person's death). Once a patient is deceased, there should be no reason for their medical records to remain accessible through MMH. Such records should be deleted from the MMH system.

This project proposes to operate on an opt-off basis, to maximise coverage for the population. A patient will be able to choose to have their record removed from MMH at a later stage.

This process would be best managed through the MMH Operational Team established for this project. The MMH Operational Team would be responsible for coordinating and ensuring a patient's record was removed from MMH. They would also be responsible for reporting back to the patient once this was done.

Should any one practice, or the PHO choose to discontinue using MMH to provide access to the SEHR for health professionals, there should be a mechanism by which patients are informed of this decision, and given appropriate opportunities to have their information removed or retained as they wish. Where a PHO or DHB chooses to discontinue using MMH, each practice should be given the opportunity to retain their patient information within MMH, while individual patients should still be able to exercise their right to have their information excluded from MMH.

If a patient moves from the district, their SEHR information within MMH should also be removed. This project covers PHO registered patients, and once a patient is no longer registered within the PHOs involved in the project, they should not have their information stored within MMH.

3.1.10 Rule 10: Use of Health Information

Rule Rule 10 limits a health agencies ability to use health information for purposes other than what it was collected for. In terms of this project, the purpose of collecting the health information is to aide in the provision of medical care to the patient.

Current Health Information is collected at present within various care settings. That information is primarily collected for the purpose of providing clinical care to the individual. It is also used for reporting on health services to health funders, almost always at an aggregated and non-patient-identifiable level. This use is outlined in patient enrolment information that the patient cites and signs every three years.

The PHO usually functions as an aggregator for General Practice and collects and reports health statistic information to funders on behalf of the General Practice. In this manner, the context of information is understood. The general practitioners hold contracts with the PHO which obligates them to supply the information and the PHO is obligated to use the information in a defined manner.

Impact The purpose of the SEHR is to provide health professionals involved in a patient's care better access to summary health information and free text of clinically subjective or objective daily records on that patient. In doing this, it is intended to allow the patient to experience improved care.

Use of patient SEHRs, by anyone other than health professionals, for any purpose other than providing direct clinical care to a patient must be explicitly forbidden. Any information required for the purposes of reporting is already collected by the PHOs, made anonymous, aggregated and reported. Allowing funders or researchers to directly report against such a data set introduces significant risk, where funders or researchers may not understand the limitations or context of the information at which they are interrogating. There is the potential for a breach of the HIPC to occur where the patient was not made aware that information may be passed onto other parties or put to a use which was not disclosed.

While the consent of the patient could be sought, this is an administratively time consuming and costly option. Therefore, a general prohibition on the use of the information for other purposes is the most workable solution.

Medtech's latest privacy statement outlines how they intend to use the information aggregated within MMH. The statement appears to be contradictory, within the first paragraph limiting the use to the purposes of the individual's healthcare and well-being. Subsequent paragraphs outline Medtech's use of the individual's health information, albeit in an aggregated form for the purposes of marketing and for providing health statistics at a population level.

Regardless of this, it will be prudent for the PHOs, on behalf of the general practices to reach a contractual arrangement that allows Medtech Limited to use the information only for the purpose of serving that information to authorised users (providers or patients) in a patient-centric summary medical record, and in an anonymous form for marketing of their product.

It should be explicitly forbidden for information contained within MMH to be used for the purposes of providing to any party population health statistics at a national or regional level. Such a process could undermine General Practice's trust in supplying information for monitoring and contractual reporting purposes. A breakdown in trust may adversely affect health professional's willingness to record and send information to MMH. This function is presently carried out through PHOs and the status quo should be maintained here. There is often a high degree of analytical processing that needs to go into providing population health statistics to ensure the highest possible level of data quality. This is particularly important when using routine clinical data that is not being recorded for population health reasons as the data often requires high degrees of normalisation and cross-checking before being presented in a reasonable form. PHOs also have mechanisms in place in which to feed information back to their member practices prior to reports being released to funders or into the public domain, as a matter of courtesy.

This rule also raises the question of the matching of data within MMH. Data matching should be done only on the patient's NHI and only for the purposes of combining health information for the purposes of providing health professionals with a clinical record. Such a scenario would be matching the health data between MMH and a secondary care system to provide both a combined primary care and secondary care record. Matching SEHR data with any agency other than a DHB, PHO, General Practice or other health care provider should be expressly forbidden.

3.1.11 Rule 11: Disclosure

Rule Rule 11 limits the disclosure of information. There are a number of scenarios in which disclosure is permitted.

Current Information collected within general practice is disclosed to other health professionals in the course of referral letters and phone conversations between treating clinicians. Patients are aware of the intent to use this information in such situations.

The health professional can make a decision at the time of disclosing the information, either in a referral document or phone call, as to what pieces of information they should disclose. They may make clinical decisions as to what parts of a patient's medical history are irrelevant to a particular referral, and choose not to disclose those items of information.

Impact The question may be raised as to whether the patient intended for the information collected to be used, to provide care outside the setting of the general practice in which it was collected. This project means only to change the mechanism by which the information is

shared, not whether it is shared or not. The 'gate keeping' mechanism for the disclosure is changed. Disclosure is currently only of a subset of information that the collecting health professional decides is pertinent to disclose to other treating health professionals. This changes because treating health professionals will have the ability to view all information contained within the patient's SEHR (that the patient has not explicitly asked to be marked as confidential or do not upload to MMH), whether it is pertinent to the referral or not.

All health professionals that are given access to this record through this project are required to be registered with a professional body. As such, they are obliged to maintain moral, ethical and professional standards at all times. This obligation should go some way to mitigate the risk of any perceived misuse of access to the whole SEHR.

In some care settings, where it is clear, an even more limited subset of information may be necessary, such as in Community Pharmacy. MMH is able to limit the view of the patient SEHR to pertinent fields. This will also protect disclosure of information not relevant in particular care settings.

For the purposes of this project, disclosure to other health professionals is permitted as the disclosure is one of the purposes in connection with which the information was collected, namely the provision of medical care to the individual. If a patient consents to treatment within a health care facility, they are, in effect, consenting to disclosure of their SEHR to health professionals treating them within that facility.

3.1.12 Rule 12: Unique Identifiers

Rule Rule 12 limits the abilities of health agencies to assign unique identifiers to patients.

Current Use of the NHI is nearly ubiquitous amongst the health sector in New Zealand, and has been so for the past 20 years. It is used on almost all paper and electronic documentation sent around the health sector as a means of uniquely identifying a patient. National Health Index numbers are assigned to patients sequentially when the patient first has contact with the health system. This results in NHIs being completely arbitrary. Because of this, some people mistakenly presume that the NHI is a way of de-identifying patient data. It is in fact the complete opposite.

Impact The MMH product will continue to use the NHI as the primary identifier for providers accessing the system to identify individuals. Determination of a patient's NHI may be through referral information, or through an appropriate system designed to search the NHI database.

In the Waikato DHB setting, for access to the patients SEHR, the primary care record will be concatenated with the secondary care system. General practice medical records will show alongside the secondary record, without the need to look-up the patient NHI. Access to the secondary system is audited, however.

Medtech's statement that email addresses will be used as a unique identifier within ManageMyHealth™ is a statement that creates uncertainty around this rule. The general intent of rule 12 is to prevent individuals from being assigned a unique identifier that can be cross-matched between various sectors and agencies. An email address can only resolve to one email account. If that email account is a personal account, it is analogous to a person. Email accounts can, however, be shared between people (perhaps in a family group) and in this case, the account is not analogous to a person but a group of people. It would be unlikely (or unwise) that an individual wishing to access ManageMyHealth™ would use an email address that resolves to an email account that is shared by other people.

3.2. Specific Considerations

3.2.1 Minors and Privacy

This section is relevant to the Patient Portal, not the SEHR as all patients' data regardless of their age will be uploaded and available on the SEHR.

Whether or not minors should have a Personal Health Record is a complex issue. This impact assessment does not present any one solution, and needs to defer any final decisions to the Clinical Workstation Governance Group.

There are currently no clear directives on how minors should be dealt with by health practitioners when it comes to informed consent for treatment and, consequently, consent to disclose their personal health information. There are both legal and ethical considerations for practitioners in this situation and, in general, decisions are encouraged to be made on a case-by-case basis.

The Guardianship Act 1968 allows people over 16 years of age to consent to health care treatment. People under 16 can consent to their own medical treatment for abortion or contraceptive advice and treatment under the Guardianship Act 1968 and Contraception, Sterilisation and Abortion Act 1977 respectively.

"The presumption that parental consent is necessary in order to give health care to children and young people under 16 is inconsistent with common law developments and the Code of Health and Disability Services Consumer's Rights 1996, a regulation under the Health and Disability Commissioners Act 1994"[13].

In an address by Kerkin in 1998 to the Consent in Child Health Workshop, Kerkin states "Parents do not have an automatic right to information about their children" and "If you would be prepared to listen to the views of a mature minor in respect to treatment, you should do the same with respect to his or her personal information [...]" [14].

In the current environment, if a patient disclosed to the health professionals that they did not wish for their health information for the visit to be shared with their parents, the health professional would likely first determine whether this was a genuine request that they would honour. It is likely that the health professional would talk this through with the patient and understand their concerns. If at the end of this process they agreed to withhold this information from the patient's parents, they would likely make a note or alert within their patient management system stating that this information isn't to be shared with anyone other than the patient.

Although practices have protocols in place to protect patient privacy, it is likely that a parent would, by ringing a practice, be able to determine if their child had a recent or up-and-coming appointment – regardless of the patient's desire to keep this confidential. This occurs usually because reception staff who would normally deal with appointment enquiries has no access to clinical portions of a patient record (for patient confidentiality reasons). In order for this to be disclosed however, the parent would already have to suspect that his or her child was attending an appointment at the practice.

If the parent wanted further details on the child's reason for the appointment or treatment, they would be required to speak to either a practice nurse or doctor. Both the nurse and doctor would likely be able to see the note to keep the patient information confidential from the patient's parents. They could at this time make another determination as to whether to disclose any further information or not (although it is likely that they would remain loyal to their initial decision to keep the contents of the consultation confidential).

In this situation, the health professional is the gate-keeper of the release of the information to any other party.

The child may take additional steps to ensure their privacy. They could visit a practice that is not their usual general practice, or visit a specific youth or school-based clinic. In these situations, the disclosure of information to the parent would likely follow the same course as for the normal practice outlined above. It would be more difficult however for the parent to know which practice to contact to speak to the relevant health professional.

Implementing the SEHR using MMH will change the dynamics of this arrangement. Parents will likely know that their child is opted on the patient-centric system. The key difference is how the parent would get access to the child's patient record. If the parent has access to the child's record via the Patient Portal then they could see all this information. In this situation, the provider has the ability to mark items as confidential or do not upload to MMH, which do not then get loaded into the MMH system. As long as the provider marks anything entered as confidential or do not upload to MMH for that appointment, the parent should not be able to see any of these items.

Children could withhold their login credentials from their parents, or choose not to have a login. This could create tensions between the child and parent or the parent could exert their power over a child to divulge their MMH login.

An alternative method would be to restrict access to the Patient Portal to those between 11 and 16 years of age. It is reasonable to assume that most children under the age of 10 wouldn't have any desire to withhold their health information from their parents. This method has problems once children age from 10 into their teenage years, where they may wish to keep certain aspects of their health care from their parents.

The current model is generally not to give children under 16 years of age access to their own Patient Portal account. They would still retain their rights under the HIPC to access information held on them, but they would be required to do this through their general practice. This would enable the health professionals responsible for the patient care to maintain the gate-keeper role. In such a situation, there would still be the potential for the parents to have information disclosed to them by the general practitioner, or by other health professionals accessing the SEHR. Such a situation is not very different from the one we currently have however.

Considerations in this section tie in closely with those in sections 3.2.2, 3.2.3, 3.2.4 and 3.2.7.

3.2.2 Opt Off Mechanisms

Patient records will be uploaded to the MMH system if they are registered in Hauraki PHO General Practices and they have not indicated that they wish to opt-out of having a SEHR. This methodology is referred to as an "opt-off" approach.

The opt-off approach has been chosen to ensure that there is maximum coverage of SEHR amongst the population from the outset of the project. Experience in other similar health systems has shown that patients choosing to specifically opt-out of such a system are extremely low. In Scotland in 2006, an emergency care summary contained records for nearly 3,300,000 patients with only 22 choosing to opt-out of the system after a public awareness campaign [15]. By 2010 the total number of patient records it held had risen to 5.4 million with 1,600 patients indicating that they wished to opt out [16].

Many people will not consider the importance of making their health information available to emergency departments, after hour's services or paramedics until they present to one of these services. By the time they present, in an opt-in system the opportunity would have been missed.

Giving patients the opportunity to opt-off of the project allows them to control how their health information is used. It does so in a way in which they must make a deliberate decision to do so, and so that they can be made aware of the consequences of not being involved in the project.

Having an opt-off methodology for such a project does increase the importance of a good public education campaign, with good patient information and a clear and easy mechanism by which patients may opt-out of the system. Obtaining widespread public awareness is not easy however. In Scotland, a direct flyer drop was undertaken to all homes as part of their Electronic Care Summary (ECS) project. Johnstone and McCartney [9] assessed people's awareness of the ECS and found that only 42 percent of patients were aware of it, and only 16 percent recognised the leaflet. In the same study, 97% of respondents, after reading the leaflet were happy for their record to be included.

3.2.3 Data Quality for Opted-Out Information

As well as a patient being able to indicate that they do not wish to have a SEHR at all, patients may also have particular information excluded from the SEHR.

Where a patient has opted-out of the project all-together, they would present to ED or an afterhours service and it would be clear to the reviewing health professional that the SEHR was not available for that patient (they would not have any information displayed in MMH). The health professional would follow the usual process of completing a history (subjective) and physical (objective) examination. They may still choose to contact patients' primary care providers to ascertain further medical detail or history for a particular patient, as they would normally do now.

Where a patient has asked for particular pieces of information to be withheld from their SEHR, it may not be obvious to a treating health professional that the record is incomplete. The patient's SEHR would be displayed in MMH, but it would not be immediately obvious that there were parts of the medical record withheld, or what parts. There could be a risk that the health professional makes a decision believing they are reviewing all the information on a patient.

This risk is mitigated in two main ways. Firstly, the SEHR is not intended to be a full patient medical record. It is intended as a summary snapshot of the patient's main medical history as recorded by the General Practice. On these grounds, it is reasonable for anyone using the SEHR to realise that it could contain significant omissions. Because of this, most health professionals using it must use it as an adjunct rather than a comprehensive record.

The second mitigation strategy is to undertake good health professional education. This should include how their practicing habits may or may not change. It should emphasise the importance of using the record as an adjunct rather than a completed record.

Recent evidence from the United Kingdom indicates that the risk of adverse incidents due to incorrect or missing information as part of a SEHR is very low [17]. Health professionals are experienced in interpreting information from multiple sources and adjust their weighting of information accordingly. This means that they are likely to account for some of the data quality issues that may arise from the use of a SEHR.

3.2.6 Access of the Patient Portal by People of Patient's Choosing

It is possible for patients to share their Personal Health Record via the Patient Portal with any person that they may choose to. Patients are able to log into MMH with their own login and password, and sit with the appropriate people in the various care settings including the patient's home and allow them to view similar information that would be available to a registered health professional through the SEHR. In this situation the carer, whānau member or advocate would not be able to access the patient's record in the patient's absence. This also provides the ability for the project to service the Whānau Ora concept in providing a degree of self-management and determination in respect to health records.

3.2.7 Ensuring Authorised Access

Any particular patient's Personal Health Record will be available to anyone with that patient's login and password (in most instances, only the patient, or in rarer circumstance, the patient's advocate or authorised family members).

The SEHR records will also be able to be located by a health professional with a user name and password login to MMH; by using the specific patient's NHI or entering in the patients demographic details such as name and or date of birth.

Only health professionals working within one of the approved care settings and who are registered will be granted logins to the system. The MMH Operational Team responsible for audits may be required to have access for the purposes of auditing and facilitating the review by a health professional of the appropriateness of patient access. Any non-clinical staff with access to MMH as part of the MMH Operational Team will be restricted to viewing only non-clinical information sufficient to enable them to undertake administrative components of tasks related to the project.

Identity verification is the key to ensuring authorised access. The Clinical Workstation Governance Group will be responsible for overseeing appropriate identity verification processes for patients and health professionals.

3.2.8 Human Rights: Stigmatisation

Many medical conditions carry stigma, including sexual health or sexual dysfunction-related conditions and mental health-related conditions. Making a patients' summary medical information available to a wider range of health professionals has been seen traditionally as potentially increasing the chance they will be stigmatised.

MMH allows patients to request that their information not be included in the SEHR by marking pertinent portions of the clinical record in the PMS as being "confidential" or "Do Not Upload to MMH". This provides some level of control to the patient.

The associated risk with stigmatisation is off-set by the ability for health professionals outside the general practice settings to be empowered with more direct information about the patient. They will be able to deliver better care to the patient providing numerous benefits.

The risks associated with not disclosing significant conditions on the summary record will need to be raised by the patients' GP at the time the request to not disclose that information is made. In the case of acute or short term conditions, such as sexual health issues, this may not be a significant concern. In the case of longer term conditions such as mental health conditions (especially where a patient is taking associated medications) this would have to be negotiated carefully.

The aspect of not having complete information about a patient within the SEHR needs to be prominent in training for health professionals.

3.2.9 Community Pharmacists Use of SEHR

In the past, the public has thought of community pharmacists primarily as being dispensers of medicines. However, they are a highly skilled health profession in their own right, with specialist skills not possessed by any other professional group. Pharmacists are often employed within PHOs to provide specialist pharmaceutical advise and to work within multidisciplinary teams undertaking medication reconciliations for complex patients.

Pharmacists interact with patients on a regular basis. Within their professional scope, they not only dispense medicine but also counsel patients.

Pharmacists have traditionally worked in an absence of patient medical record information. Usually the only information they work with are the prescriptions they are presented with, and any information that the patient is able to volunteer – usually a lay description of the ailment that they are being treated for. The pharmacist is an important safety mechanism in the process of prescribing medications. In providing a segregation of duties between prescribing and dispensing they are an additional check that any obvious medication errors, particularly relating to transcription or dosage have an additional chance of being detected.

Giving community pharmacist's access to a patient's SEHR, with the patients consent, is one way of improving the information that pharmacists are able to work with when checking prescriptions. Currently, this would initially be done with a check with the patient or basic information as to their condition or treatment and with a communication with the prescribing health professional, usually the patient's general practitioner, if warranted.

Having an SEHR changes the ability of the pharmacist to access information. The GP would no longer be the gatekeeper of this information. The nature of pharmacist's interactions with patients is different from other health professionals. With other health professionals, patients usually present to a clinic for the purpose of being assessed and possibly treated by the health professionals there. In a community pharmacy setting, where retail as well as professional services are provided, this may not necessarily be the case. Patients may go to a pharmacy for retail services, and end up interacting with a pharmacist without even being aware of the distinction between pharmacy assistants and pharmacists.

It will be important for pharmacists to make a clear distinction between when a patient presents for retail versus professional services. Presentation of scripts for dispensing, and consulting pharmacists for health advice may be two situations where it is appropriate for a pharmacist to access the SEHR.

General Practices are not the only prescribers of medicines. The SEHR, within the scope of this project, will only include information from a patient's general practice. Pharmacists will need to be well educated to ensure that they are aware that any prescribing list will only be part of the patient's prescribing record.

3.2.10 Project Scope Change

Projects over time are subject to change and modification. This is usually done to improve outcomes or decrease expenditure. This privacy impact assessment is outlined for the project in its current configuration. Although the intent is to deliver the project outlined, it is conceivable that some operational details or objectives may change.

The Clinical Workstation Governance Group is the structure that will be used to have oversight of the project, with particular regard to privacy. This group will be responsible for endorsing any significant proposed change in the project, from initial planning to ongoing operation.

3.2.11 General Practice Opt-In

The primary care information infrastructure is complex in its nature. Generally, each general practice owns and maintains its own practice management system. This system not only contains patient records, but also runs the administrative and financial functions for the practice.

In order for a practice to contribute information to MMH to be used as a SEHR, each practice must have activated the routines that upload data to MMH.

Through extensive health professional education, it is expected that the majority will understand the enormous benefit that a SEHR will be able to provide to patients. It is expected that very few practices would initially opt to not offer this service for their patients.

For those practices that have clinical or other concerns, Hauraki PHO Clinical Leadership will engage with those practices to ensure that they make informed clinical decisions to opt-out of the project.

Patients that wish to have a SEHR but who are registered at a practice that may have chosen to opt-out of the project will not be able to have a SEHR.

It is possible that any general practice may wish to discontinue their involvement in the project after the initial recruitment phase;

- When a practice that is already on the SEHR decides to opt out, Medtech will mark the practice as having opted out of the SEHR and all of the patient records for this practice will be made inactive. These records will no longer be available to be viewed on the SEHR.

In all of the above cases, where a patient or practice opts out, Medtech will retain the data for the minimum period of 10 years as per the "Health (Retention of Health Information) Regulations 1996"[3]. After this minimum retention period has lapsed all data is deleted.

In a situation where a practice chooses to opt of the SEHR, it will be important for the practice to ensure that they inform patients of their intent to withdraw from the project; as withdrawal will also have an impact on how the patient's information is used (or not used, as the case may be).

3.2.12 Ownership and Intellectual Property

Patients have rights over their health information as well as rights of access and correction to information about themselves. Health Professionals have obligations over the health information they hold[4]. They also have a duty of care to ensure that information is stored securely and, in maintaining continuity of care to patients, is shared appropriately.

PMS vendors own the intellectual property for the systems that are used to store the information, including the database structure that is used to store the information. The data that is contained within these systems however is still owned by the patient.

There is a clear distinction between the data contained within a system, and the technical data structures that are used to store and serve that data.

MMH presents no significant change from this concept. The patient and health professional still own the health data that pertains to them, while Medtech Limited retains the intellectual property of the MMH system.

3.2.13 Patients with Impaired Decision Making Capability

There are two aspects of consideration in the way in which patients with impaired decision making abilities are dealt with which are:

- the decision to opt-out of the project; and
- consent for health professionals to view the SEHR.

The decision to opt out of the project is a decision that will affect those that have an impaired decision making capability for an extended period of time. This may include those with degenerative conditions or severe head trauma, but is unlikely to include those that are temporarily unconscious.

---

[3] http://legislation.govt.nz/regulation/public/1996/0343/latest/DLM225650.html?search=sw_096be8ed814ff4a1_retention+period_25_se&p=1

[4] https://privacy.org.nz/news-and-publications/guidance-resources/health-information-privacy-fact-sheet-1-overview/

Patients who have impaired decision making for extended periods may have a power of attorney in place, advanced care plan or their next of kin may have the ability to make decisions about their health care on their behalf. In these situations, the person who would normally be able to act for the patient in regard to informed consent should also be the person that is responsible for the decision whether to opt the patient out of the SEHR or not.

For such people, they may register their wish to opt the patient out of the project in the same way as a patient would. As per clause 2 of the HIPC, they will need to confirm they are the parent or guardian of a child under 16, the executor of the estate of a deceased person or someone lawfully acting on behalf of someone who cannot give consent or exercise their rights. Patients often present in care settings such as the Emergency Department and Aged Care facilities where their decision-making ability is impaired to some degree (they may be unconscious or confused). In these situations, it may not be practical for treating health professionals to ask for the patient's consent to view their SEHR. Health professionals who are making a decision to treat a patient in such a situation should also have the capacity to access the patient's SEHR without the explicit consent of the patient. This will be documented in the patient's record.

3.2.14 Use of Medtech32 and Medtech Evolution Confidentiality and Do Not Upload to MMH Flag

Currently, data items that may be uploaded to MMH can be marked with a "confidentiality" or "Do Not Upload to MMH" flag within Medtech32 and Medtech Evolution. Traditionally the confidential flag was not intended for use with MMH, and is generally used by General Practice 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 being proposed that these flags be used to provide a level of granularity around what information about each patient is able to be viewed through the SEHR. By marking individual items as "confidential" or "do not upload to MMH" those particular items would not be included in the SEHR, while the remainder of the patient record would.

The Clinical Workstation Governance group have recommended that clinicians make patients aware that they can ask for aspects of their health information to be withheld from the SEHR, with the understanding that withholding information may make their care more difficult at a later time.

4. Recommendation Summaries

The Clinical Workstation Governance group will review one section of these recommendations at each governance meeting.

4.1. Opting Out

#	Description	Impact Reference
1	It must be easy for patients to indicate that they wish to opt-out of the project.	There should be no barriers for patients to choose to not have their information included in a SEHR within MMH.
2	Patients should be able to present to their General Practice and indicate that they wish to opt-out of the project.	Patients must be able to make an informed choice about what happens to their health information. Some patients may not have access to a telephone to opt-out over the phone.

4.2. Patient Education

#	Description	Impact Reference
1	Public awareness campaigns should be run within the geographical regions for Hauraki PHO.	The way in which information moves around the health sector will change. Patients need to be aware of what is going to happen to their health information (Rule 3).
2	Patient information contains very clear and explicit instructions on the importance of keeping their personal username and password for ManageMyHealth™ Patient Portal. This also needs to outline appropriate circumstances in which they could give their login information to a parent, guardian or caregiver.	Patients will have the ability to access their own Personal Health Record. Because of this, they also have the ability to inadvertently provide access to their Personal Health Record if they disclose their username and password to a third party. To maintain the security and confidentiality of their information, they must keep this username and password private (Rule 5).
3	Patient should be advised they are able have or have data withheld at a granular level from the SEHR	Patients must be able to make an informed choice about what happens to their health information. They must be able request certain parts of their health information is withheld from the SEHR

4.3. Provider Education

#	Description	Impact Reference
1	Health professionals should be given clear messages in training that the SEHR should only be used in conjunction with standard history taking methodologies, and should not be relied on by itself.	The SEHR is only a summary record. It is intended as an adjunct to good clinical practice. Omission of vital information from the SEHR may occur for various reasons. Health Professionals must not rely on the information within SEHR alone (Rule 8).
2	Training of health professionals need to include aspects of how a SEHR may affect patient stigmatisation compared with traditional models.	The SEHR may contain information that may contribute to patient stigma, particularly around sensitive information such as Mental Health or Sexual Health-related matters.
3	Health Professional education and training material emphasises the importance of keeping their username and password safe and secure, not sharing logins and reporting immediately any time where their username or password may have been compromised.	Health Professionals will have the ability to access patient SEHRs. Because of this, they also have the ability to inadvertently provide access to the SEHR to others if they disclose their username and password to a third party. To maintain the security and confidentiality of their information, they must keep this username and password private (Rule 5).
4	Health professionals should be educated where in the circumstance that they base significant clinical decisions on information obtained through the SEHR, especially where that decision is influenced contrary to what they may otherwise have made in the absence of the information, that they should document within their own notes the information that caused them to make this decision. They must be aware that the aggregated record is mutable.	The SEHR is an aggregated record. It is sourced from other patient records that may be changed over time. While the accuracy of the SEHR is paramount, it is mutable by its very nature. The SEHR may also be incomplete. It is possible for clinical decisions to be based on information within the SEHR, but for that SEHR record to not persist.
5	Health professionals wishing to access a patient's SEHR should routinely ask patients for consent to view their shared record. Where patients are not able to give such consent or where consent has been previously obtained from that patient (they may be unconscious or otherwise incapacitated), such consent should be bypassed.	Gaining verbal consent to access the SEHR and documenting this in the patients record gives patients who may not otherwise be aware that their record is accessible in a care setting to determine whether they wish for it to be accessed.
6.	Health Professionals should be educated to advise patients they are able to opt off either completely from the SEHR or have data withheld at a granular level from the SEHR	There should be no barriers to patients opting off the SEHR or for patients to request the ability to withhold information from the SEHR at a granular level

4.4. Manage My Health Functionality

#	Description	Impact Reference
1	MMH should allow a patient to attach a note disputing the accuracy of information if their request for update of information is declined by a general practice. Providers should also have some ability to make seen within MMH a note to the same effect if requested to do so by the patient.	Any disputes over accuracy of information may be recorded in normal general practice within the clinical note. Patients that wish to dispute the accuracy of information that the health professional does not wish to correct must have some way of flagging such information is in dispute by them.
2	There should be a mechanism by which the MMH Operational Team is able to confirm the presence of a patient's SEHR within MMH.	
3	The SEHR should remove or make inaccessible a patient's medical record once it is confirmed the patient is deceased.	Information should only be retained as long as it is needed. As MMH is not intended to be used for medico-legal purposes, a patient's health information should be removed from their SEHR upon their death. A record would be retained in General Practice indefinitely (Rule 9).
4	The ManageMyHealth™ privacy statement should remove from its limits of use clause, the intention to use the information within ManageMyHealth™ to provide population health statistics data at a national or regional level. This should be re-enforced with any contractual arrangement with Medtech Limited	Information provided to MMH for inclusion in the SEHR if used for anything other than direct clinical use could cause patients or providers to withhold information.

4.5. Processes and Practices

#	Description	Impact Reference
1	Organisations providing access to health professionals should be required to have within their employment contracts appropriate sections that label actions that breach network security or patient privacy as serious misconduct.	The "surface area" for attack of the MMH product is greater than information stored within existing General Practice. A breach in the security of one system could compromise a whole district's patient's health information.
2	The Clinical Workstation Governance Group or other appropriate clinical group should work to establish guidelines for use of the SEHR within community pharmacy settings, before access is granted to MMH in these settings.	General Practitioners and patients may perceive it to be unnecessary for some care settings to view the whole SEHR – specifically community pharmacy settings.
3	The Clinical Workstation Governance Group should ratify an appropriate process to support providers' requests to prevent patient access to their own Personal Health Record on the grounds outlined in HIPC rule 6.	Health Professionals may need to prevent their patients accessing their own medical records in accordance with the Privacy Act. The patient having access to their own records means that the traditional "gate keeper" role played by the GP will no longer apply.
4	Appropriate identity verification processes need to be implemented, so that patients wishing to opt-out, request information held within their medical record, or request an access audit can be verified as truly being the patient.	Patients, while known to General Practice, are not known to the PHO on a personal level. The PHO must ensure the identity of a patient before proceeding.
5	Data contained within MMH should not be matched for any purpose, other than with another health agency providing direct clinical care to a patient, for the purposes of providing a combined clinical record.	The SEHR provides easy central access to NHI based information on patients. This makes the information valuable for matching. Matching the data within MMH for a purpose other than providing direct clinical care to individual patients could make patients and health professionals not want to contribute information to the SEHR.
6	Data matching for the purposes of providing a combined clinical record, for direct clinical care should only be matched on a patient's NHI.	
7	All processes and practices should be included within an operational guidelines document. This document should become the living document for the project. Changes to this document should be endorsed by the Clinical Workstation Governance Group.	There are a number of processes and procedures that need to be developed, ratified by the Clinical Workstation Governance Group and implemented by the MMH Operational Team. These processes will be varied and need to be implemented accurately to ensure the individuals maintain the privacy of their information.

8	Practices, PHOs and DHBs may choose to discontinue using MMH to provide access to SEHR. In this situation, a process must be set up that enables patients registered within the practice, PHO or DHB to have their information removed from MMH.	Rule 9 : Retention

4.6. Non-participating Care Settings

#	Description	Impact Reference
1	Health services that do provide detail to the SEHR prominently display information that makes this clear. All services that do so should have patient education information in a prominent and accessible place.	Patients need to be aware of what happens to their health information. Implementing MMH and a SEHR changes the information flows within the sector. Patients need to be informed what happens to their information so that they can make appropriate decisions about it.
2	Organisations with staff accessing the MMH system will be required to ensure that the employment agreements that they have with their staff have clauses that treat the breach of security to patient systems as serious misconduct.	The SEHR will be a system where patient records can be accessed by health professionals within a number of organisations. It is important security if maintained within each and every organisation. It is possible that staff will not utilise MMH appropriately – putting the privacy of all those on the system at risk. All Hauraki PHO practices have or are in the process of obtaining Cornerstone Accreditation.
3	Organisations will also be asked to ensure that their network and processes and procedures meet a minimum security standard (based on HISO's recommendations[12])	The SEHR will be a system where patient records can be accessed by health professionals within a number of organisations.
4	A Governance team comprising members of Hauraki PHO, WDHB, practice representatives and consumers will be established and maintained.	Access to the SEHR will be relatively open to health professionals within approved care settings. Some restricted rights will be applied in some care settings, such as community pharmacy. In general, procedures and processes will ensure the on-going appropriate use of the system by all. Processes need to be implemented by appropriate staff.

5	The MMH Operational Team will facilitate regular audits of provider access to patient records on the system. Where an investigation needs to be made, this will be done by appropriate health professionals. Any finding from an investigation that shows a breach of privacy will be reported this to the offender's employer.	Access to the SEHR will be open to health professionals within approved care settings. Some restricted rights may be applied in some care settings, such as community pharmacy.
6	The MMH Operational Team will, prior to the establishment of the aggregated shared record, set up and be responsible for a process to answer patient queries around access to their records, and when requested on behalf of the patient facilitate the investigation of the appropriateness of this access. Only health professionals will have access to clinical information as part of any such investigation. The process will require reporting back to the patient the outcome of any investigation.	

5. Project Governance

The following is the suggested composition of the governance structure for the SEHR.

The Clinical Workstation Governance Group will have representation from patients and consumers, clinicians, privacy officers, information professionals and it will be the responsibility of those representatives to interface and present the issues of their respective constituents. Such governance structures for electronic health records project is supported internationally [18].

The functions of the governance group will include[5]:

- Provide Project Data Governance
- Policy and Procedure Oversight
- Appointment of Clinical Auditors Where Necessary
- Review of Privacy Audits and Outcomes
- Control of Project Expansion or Significant Change

The governance group will be directly accountable to the HPHO Board of Trustees and Hauraki Hauora Alliance Leadership Team. The group will be established in its own right, rather than as a sub-group of any other established committee or board as the project has such significance, profile and specific subject matter.

It will be expected that representatives of the group are well informed by their constituents within the wider health sector, and that they bring representative views for discussion.

The MMH Operational team will be responsible for implementing and executing the policies and procedures decided upon by the Clinical Workstation Governance Group. The MMH Operational team will be made up of resources, most likely from the PHO. They will also be able to call on, from time to time and where appropriate technical resource from within primary or secondary care.

[5] 281016 Hauraki PHO MMHCWGG Terms of Reference Final

6. SEHR and MMH Terminology

The terminology used in this document tries to distinguish between a SEHR and MMH. The Shared Electronic Health Record is used to describe the generic concept of aggregated patient data, while MMH describes the proprietary technology with which the patient data is accessed and presented

Figure 7 below shows on the left how MMH and the SEHR are related in the current configuration. They are currently tightly coupled. The MMH data repository is the SEHR data repository

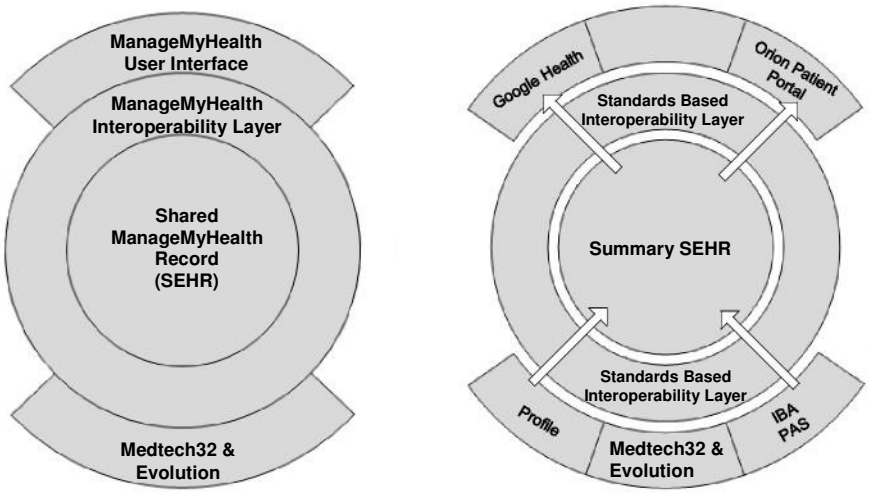

Figure 7: Current (left) and Future (right) relationships of SEHR and MMH

7. Description of Agencies

Agency	Description
Ministry of Health	Government agency responsible for setting health policy.
Hauraki PHO	The PHO that supports our enrolled population and other eligible persons to stay well and ensure they receive accessible, quality, coordinated care delivered by multi-disciplinary teams.
Hauraki PHO CAG	Hauraki PHO Clinical Advisory Group
Hauraki PHO Clinical Workstation Governance Group	Hauraki PHO ManageMyHealth™ and Clinical Workstation Governance Group
Waikato DHB	District Health Board responsible for the provision of health services in the Waikato region
Medtech Limited	A private software vendor, that products the Medtech32 and Medtech Evolution Practice Management System, and ManageMyHealth™

8. Glossary of Abbreviations

Abbreviation	Description
CWS	Waikato DHB Clinical Workstation
HIPC	Health Information Privacy Code
MMH	Manage My Health
MSO	Management Service Organisation
OPC	Office of the Privacy Commissioner
PHO	Primary Health Organisation
PMS	Practice Management System
SEHR	Shared Electronic Health Record

9. Health Information Privacy Code 1994 Rule Summary

The following list summarises the 12 rules that constitute the Health Information Privacy Code 1994[6]. Each rule governs a particular aspect of health information privacy, which is listed above a basic explanation of the consequence of applying the rule. Both are taken directly from the commissioner's publication.

Rule 1:	Purpose of collection of health information. Only collects information if you really need it.
Rule 2:	Source of health information. Get it straight from the people concerned.
Rule 3:	Collection of health information from individual Tell them what you're going to do with it.
Rule 4:	Manner of collection of health information – be considerate when you're getting it.
Rule 5:	Storage of and security of health information. Take care of it once you've got it.
Rule 6:	Access to personal health information. People can see their health information if they want to.
Rule 7:	Correction of health information. They can correct it if it's wrong.
Rule 8:	Accuracy etc. of health information to be checked before use. Make sure health information is correct before you use it.
Rule 9:	Retention of health information. Get rid of it when you're done with it.
Rule 10:	Limits on use of health information. Use it for the purpose you got it.
Rule 11:	Limits on disclosure of health information. Only disclose it if you have a good reason.
Rule 12:	Unique identifiers. Only assign unique identifiers where permitted.

[6] Health Information Privacy Code 1994: Incorporating amendments and including revised commentary. Privacy Commissioner. December 2008.

10. ManageMyHealth™ Privacy Statement

This information was taken from the Manage My Health website, and has been indicated as being last updated on Friday, January 1, 2010.

Note that this section (from 10.1 onward) is reproduced from the Medtech website. It is Copyright © 2008 ManageMyHealth™. All Rights Reserved. Heading numbering has been added to conform to this document's layout and reference structure. No other changes have been made to the text.

10.1. Introduction

Medtech Limited is committed to protecting your privacy through its SEHR information technology service, *ManageMyHealth™,* and its strict adherence to privacy laws. Medtech Limited is also referred to as "Medtech", "we" and "us" in this statement and when referred to, such reference includes any person or organisation to which it has licensed or assigned its rights and obligations.

This Privacy Statement applies to the use of the *ManageMyHealth™* site at www.managemyhealth.co.nz ("*ManageMyHealth™*") and the data collected by Medtech through *ManageMyHealth™*

ManageMyHealth™ is a personal health service that lets you review, gather, edit, store, and deal with health information online. With *ManageMyHealth™* you have the ability to access your own medical records if your medical practitioner makes these available through *ManageMyHealth™*. You can also share your health information with family, friends, and health care professionals, and have access to online health information management tools.

You can choose to share specific information (or all information); with other people (such as friends and family) and with applications (such as applications that add data to your health records, provide information to your healthcare provider, or use some of your health records to provide information to you about managing your health).

ManageMyHealth™ also provides information on well-being generally and incorporates contributions from third parties.

This Privacy Statement is in two parts, Part A deals with Privacy generally and Part B specifically addresses the Health Information Privacy Rules prescribed in the New Zealand Health Information Privacy Code 1994 (as amended) published by the New Zealand Privacy Commissioner.

By using *ManageMyHealth™* you agree to be bound by this Privacy Statement and the Terms of Use.

10.2. Part A – General Privacy Statement

10.2.1 Collection of your personal information

The first time you sign in to *ManageMyHealth™*, *ManageMyHealth™* asks you to create an account. To create an account, you must provide personal information such as name, date of birth, e-mail address & physical address.

We may request other optional information, but we clearly indicate that such information is optional. You can review and update your account information. You can modify, add, or delete any optional account information by signing into your *ManageMyHealth™* account and editing your account profile.

An account allows you to manage one or more health records, such as the ones you create for yourself and your family members. You can choose what information to put in your records.

To access your medical records held by your participating Healthcare Provider an activation code must be obtained in person from the Healthcare Provider. One specific e-mail address must be provided along with a valid photo-id.

You can close your account at any time by signing into your *ManageMyHealth™* account and editing your account profile. We wait 90 days before permanently deleting your account information and all records.

10.2.2 Storage of information

Any information or records you maintain with a *ManageMyHealth™* account will be hosted on servers in a SEHR environment by a commercially reputable hosting vendor using best practice security techniques.

If you choose to access your medical records held by your medical practitioner through *ManageMyHealth™* you are consenting to *ManageMyHealth™* storing that information on your behalf and obtaining periodic updates to the records via your Healthcare Provider.

10.2.3 Security

When any information is uploaded to your *ManageMyHealth™* account, it sends it over the Internet using SEHR Sockets Layer (SSL). This method encrypts the information to help prevent others from reading it while it's in transit from your computer to *ManageMyHealth™*.

The health information held is encrypted within the *ManageMyHealth™* database. Further information about the security measures used is contained under the heading Rule 5 – Storage and Security of Health Information in Part B of this statement.

If you're using *ManageMyHealth™* to upload sensitive data, you should properly SEHR your computer. To help do this, you can use anti-spyware and virus protection software. You can also restrict access to your computer (for example, by using a strong password for your computer login and a network firewall).

Medtech has incorporated all reasonable measures to protect your information; however, we are reliant upon you to do the same.

Medtech cannot be held liable in any way for events beyond our control or in any way for accidental or unauthorised access of your information.

Accidental access could be obtained by leaving yourself logged on and leaving your computer unattended, 'over-the-shoulder' access or from unsecure print-outs of your information.

Unauthorised access could involve someone who is known to you guessing your password or a stranger/hacker circumventing our security measures. Social engineering is the easiest way to achieve unauthorised access to your information. To prevent this never give your access details to anyone, this includes your password.

10.2.4 Sharing your personal health information

A feature of *ManageMyHealth™* is the ability to share your health information with people and services that can help you manage your health or meet your health-related goals.

You can share information in a *ManageMyHealth™* account with another person or business through *ManageMyHealth™*.

10.2.5 How we may use your personal information

Medtech collects and uses your information to operate and improve and deliver *ManageMyHealth™* or carry out the transactions you have requested. These uses may include providing you with more effective

customer service; making *ManageMyHealth™* or its services easier to use by eliminating the need for you to repeatedly enter the same information; performing research and analysis aimed at improving our products, services and technologies; and displaying content and advertising that are customised to your interests and preferences.

Medtech may occasionally hire other companies to provide services on our behalf, such as web site hosting; packaging, mailing; answering customer questions about products and services; and sending information about our products, special offers, and other new services. If we provide personal information to such companies, we only provide the personal information they need to deliver *ManageMyHealth™* product and services. They are required to maintain the confidentiality of the information and are prohibited from using that information for any other purpose.

Medtech may disclose personal information if required to do so by law or in good faith believe that such action is necessary to: comply with the law, comply with legal proceedings served on Medtech or *ManageMyHealth™*; protect and defend the rights or property of Medtech and our family of web sites; or, act in urgent circumstances to protect the personal safety of users of Medtech products or members of the public.

10.2.6 How we use aggregate information and statistics

Medtech may use aggregated information from *ManageMyHealth™* to improve the quality of *ManageMyHealth™* and for marketing of *ManageMyHealth™*. This aggregated information is not associated with any individual account. Medtech does not use your individual account and record information from *ManageMyHealth™* for marketing without Medtech first asking for and receiving your opt-in consent.

10.2.7 Record access and controls

When you create a record, you become the person responsible for that record. You decide what level and degree of access to grant other users of your *ManageMyHealth™* records. You can view and update records you are responsible for and can examine the history of access to those records.

10.2.8 Sharing records with applications through ManageMyHealth™

We may provide you with information about applications that connect with *ManageMyHealth™*. You can view the applications and should examine their privacy statements and terms of use prior to using them or allowing them access to any of your health information. In order to access *ManageMyHealth™*, the application provider must commit to protecting the privacy of your health data.

No application has access to your information through *ManageMyHealth™* unless and until you opt in through *ManageMyHealth™* to grant it access. You control what health information you allow an application to access and the length of time they can access the information.

10.2.9 E-mail controls

To keep you informed of the latest improvements, *ManageMyHealth™* will send you a newsletter. By creating an account you have given us your implied consent to send you such newsletters. If you do not want to receive the newsletter, you can unsubscribe at any time.

10.2.10 Use of cookies

We only use temporary cookies on *ManageMyHealth™* which are deleted upon you signing out. The cookies contain no personal information.

10.2.11 Changes to this privacy statement

We may occasionally update this privacy statement. When we do, we will also revise the "last updated" date at the top of the privacy statement. We encourage you to review this privacy statement periodically to stay informed about how we are helping to protect the personal information we collect. Your continued use of *ManageMyHealth™* constitutes your agreement to this privacy statement and any updates.

10.2.12 Enforcement of this privacy statement

Medtech must comply with privacy legislation when dealing with personal information. If you would like any further information or have any queries, problems or complaints relating to our Privacy Policy or our information handling practices in general, please contact us at:

Privacy Officer
ManageMyHealth™
PO Box 3329
Shortland Street
Auckland 1140

Email: privacy@managemyhealth.co.nz

10.3. Part B – Compliance with the Rules contained in the Health Information Privacy Code

The New Zealand Health Information Privacy Code 1994 as amended modifies the privacy rules contained in the Privacy Act 1993 as they relate to health information. Each of these rules is addressed below.

10.3.1 Rule 1: Purpose of Collection of Health Information

Information is collected and maintained for individuals for the purpose of improving or maintaining their health and well-being. Use of the information for other purposes is not authorised. Express consent must be given by the individual if the information is used for any other purpose.

Aggregated information which has identifying information removed may be used to improve the quality of the services offered on *ManageMyHealth™* for marketing of *ManageMyHealth™* and for general analysis or population health statistics.

Medtech does not use your individual account and record information from *ManageMyHealth™* for marketing without Medtech first asking for and receiving your opt-in consent.

Any information submitted to *ManageMyHealth™* Community Forums or Blogs becomes public information and is not covered by this privacy statement. Accordingly you should be cautious as to what personal information you supply in these areas.

10.3.2 Rule 2: Source of Health Information

The source of the information will come directly or indirectly from you.

This includes the information you authorise to be supplied by your doctor or other health professional.

Medtech has no control over the content of the information which is provided to you by your Healthcare Provider or other authorised third parties.

10.3.3 Rule 3: Collection of Health Information from

Individual

Information submitted to *ManageMyHealth™* for collection must be specifically authorised by the individual.

Subsequent access to the information by third persons (such as health care professionals and family members) will only be accessible by those persons the individual specifically authorises to have such access.

10.3.4 Rule 4: Manner of Collection of Health Information

The collection of information will always be undertaken in a manner that is lawful and with the specific authorisation of the individual.

Information entered by an individual (or on behalf of an individual e.g. minor in their care) is entirely at their discretion.

If Information is provided on behalf of an individual, it is assumed the provider has the legal right to do so.

10.3.5 Rule 5: Storage and Security of Health Information

Storage of information is hosted in a SEHR environment by a commercially reputable hosting vendor using best practice security techniques.

The information is encrypted within the *ManageMyHealth™* database.

Information delivered to *ManageMyHealth™* from your Healthcare Provider is encrypted during transmission. Your information provided to you via a web browser is encrypted during transmission using the highest standard available today using VeriSign Digital Certificates. This provides at least 128 bit encryption or 256 bit encryption if you are using the latest version of the web browser.

ManageMyHealth™ is protected by a reputable network Firewall.

Daily Backups are performed to allow system restores to be performed in a disaster recovery situation.

Access to your account will be blocked following 5 failed attempts to logon. Your account is unblocked by using the forgotten password function on the website.

Information provided to you from your Healthcare Provider cannot be modified within the system.

Medtech follows strict internal procedures in collecting, storing and disclosing information about you.

10.3.6 Rule 6: Access to Personal Health Information

We will act reasonably to ensure you will have access to your information at any time.

The exceptions to this include:

- You have been denied access to *ManageMyHealth*™;
- *ManageMyHealth™* requires a planned outage;
- *ManageMyHealth™* experiences an unplanned outage. Such events are considered beyond our control but all reasonable efforts will be used to re-establish the service as soon as possible.

We offer no guarantees that access to your information is available at all times.

10.3.7 Rule 7: Correction of Health Information

Information entered by you can be modified at any time.

If you do modify your information you must consider what impact that may have on a person authorised by you who may have previously read the information and potentially acted on it. If this impact is significant you should inform the individual of the change.

All other information about you provided by authorised third parties cannot be modified by *ManageMyHealth*™. If you feel information requires correction you must contact the information source and request a correction. *ManageMyHealth™* has no control of or responsibility for this process or the outcome.

10.3.8 Rule 8: Accuracy etc. of Health Information to be Checked before Use

All reasonable steps are taken by *ManageMyHealth™* to ensure the information submitted is accurately stored.

Human error (either by *ManageMyHealth™* staff and agents, by you or any third party submitting information) cannot be easily identified by *ManageMyHealth*™. Therefore, before using any information all users must take such steps as are reasonable in the circumstances to determine its accuracy.

Users must not act if the information appears incorrect.

If any user acts without taking reasonable steps to determine its accuracy that user is responsible for their actions and not necessarily the person who provided the information.

It is important you maintain the accuracy of your contact information so that you can be contacted at any time.

10.3.9 Rule 9: Retention of Health Information

Medtech will not delete your information unless your access is terminated.

If your account is blocked because you have abused your access privileges you will be offered the opportunity to obtain a copy of any legitimate health information you have entered. In these circumstances information provided by your Healthcare Provider will not be provided and must be obtained from your Healthcare Provider.

10.3.10 Rule 10: Limits on Use of Health Information

Access to your information by you and others is limited to the purpose of your healthcare or well-being. Use outside of this purpose is not permitted without authorisation.

Our terms and conditions authorise use of aggregated information which has identifying information removed. This aggregated information may be used to improve the quality of the services offered on *ManageMyHealth*™, for marketing of *ManageMyHealth™* and for general *ManageMyHealth™* usage analysis or population health statistics.

Health statistics will be gathered to allow planning of effective healthcare services within your region. This information is extremely valuable as it allows the limited healthcare services to be targeted to the needs of the population, which in turn potentially provides benefits to you and your family.

Medtech does not use your individual account and record information from *ManageMyHealth™* for marketing without Medtech first asking for and receiving your opt-in consent.

10.3.11 Rule 11: Limits on Disclosure of Health Information

Initially access to your information will be limited to you and your registering doctor, including other doctors within your doctor's practice. This will be expanded in later versions to other health professionals you authorise and an optional "trust list" functionality which will allow you to grant access to other individuals involved with your care.

Medtech may occasionally hire other companies to provide services on our behalf, such as web site hosting; packaging, mailing; answering customer questions about products and services; and sending information about our products, special offers, and other new services. If we provide personal information to such companies, we only provide the personal information they need to deliver *ManageMyHealth™*. They are required to maintain the confidentiality of the information and are prohibited from using that information for any other purpose.

Medtech may disclose personal information if required to do so by law or in good faith believe that such action is necessary to: comply with the law, comply with legal proceedings served on Medtech or *ManageMyHealth™*; protect and defend the rights or property of Medtech and our family of web sites; or, act in urgent circumstances to protect the personal safety of users of Medtech products or members of the public.

We will not otherwise disclose such of your information that allows you to be identified to anyone without your consent.

10.3.12 Rule 12: Unique Identifiers

The primary unique identifier used within *ManageMyHealth™* is an email address of your choice, which you have authorised us to use to communicate with you. This identifier may be linked to your National Health Index number, if known, which is allocated to you when you use a service provided by a New Zealand District Health Board such as a public hospital. No other unique identifier is linked to you by *ManageMyHealth*™.

While an email address is globally unique we cannot guarantee that it will always be assigned to the same person. If an email address is no longer used by an individual it is then typically 'made available' to anyone else who wants to use it, much the same as a phone number. In the case of children we allow the use of a parents email address. Once an individual becomes 16 years old they become responsible for maintaining their account access by other persons such as their parents.

We are aware that over time you may change your email account hence you are allocated a unique system identifier which is inaccessible except by the system.

12. References

1 Ministerial Review Group: Meeting the Challenge: Enhancing Sustainability and the Patient and Consumer Experience within the Current Legislative Framework for Health and Disability Services in New Zealand. Ministerial Review Group; 2009.

2 Health Information Strategy Steering Committee: Health Information Strategy for New Zealand. Ministry of Health; 2005.

3 National IT Health Board: National Health IT Plan : Draft For Discussion. National IT Health Board; 2010.

4 Simpl: Health Management System Collaborative: Report for DHB Boards for April 2009. Simpl; 2009.

5 Wave Advisory Board to the Directory General of Health: From Strategy to Reality: The WAVE Project. Ministry of Health; 2001.

6 Office of the Privacy Commissioner: Privacy Impact Assessment Handbook. Office of the Privacy Commissioner; 2007.

7 Manawatu PHO, Horowhenua PHO, Otaki PHO, Tararua PHO, MidCentral DHB, Compass Health: Transforming Primary Health Care Services: MidCentral Business Case 2010.

8 Wairarapa Community PHO, Wairarapa DHB, Compass Health: Tihei Wairarapa: Business Case for Primary Health Care in the Wairarapa. ; 2010.

9 Johnstone C, McCartney G: **A Patient Survey Assessing the Awareness and Acceptability of the Emergency Care Summary and its Consent**. Perspectives in Health Information Management 2010, **Spring**: 1-10.

10 Morris L, Cameron J, Brown C, Wyatt J: **Sharing Summary Care Records: Results from Scottish Emergency Care Summary**. BMJ 2010, **341**:C4305.

11 Privacy Commissioner: Health Information Code 1994. Privacy Commissioner; 2008.

12 Health Information Standards: Health Information Security Framework Essentials and Recommendations: HISO 10029.1. Ministry of Health; 2009.

13 Ministry of Health: **Consent In Child and Youth Health: Information for Practitioners**. 1998.

14 [http://www.privacy.org.nz/disclosing-children-s-health-information-a-legal- and-ethical-framework/]

15 Watson N: **Patients should have to opt out of national electronic care records: For.**. BMJ 2006, **333 (7557)**:39-40.

16 **Emergency Care Summary** [http://www.slideshare.net/sanidadyconsumo/emergency-care-summary]

17 Greenhalgh T, Stramer K, Bratan T, Byrne E, Russell J, Potts H: **Adoption and non-adoption of a shared electronic summary record in England: a mixed-method case study.**. BMJ 2010, **340**:c3111.

18 Reti S, Feldman H, Safran C: **Governance for Personal Health Records**. Journal of the American Medical Informatics Association 2009, **16**:14-17.