Privacy Impact Assessment

Compass Health – Patient Portal

5 November 2015

Table of contents

Executive Summary

1. This privacy impact assessment involves a review of the planned implementation of the ManageMyHealth™ patient portal to general practices across the Primary Health Organisations in the Central Region. It provides an introduction and overview of the proposal and then considers the relevant privacy principles in the collection, storage, use and disclosure of personal information that arises from the proposal in order to make some key recommendations.
2. The key recommendations are:
    a. To ensure that there is clear governance with proper management flowing from that governance.
    b. The agencies involved in the implementation of the portal must ensure clear agreements are in place between them as to their individual obligations/responsibilities to ensure privacy and confidentiality of the health data.
    c. The participating general practices and Medtech need ongoing vigilance against operational security risks, including ongoing staff training, system monitoring and auditing of access and use of the portal.
    d. Enrolment for access to the portal will show patient consent and understanding of the risks of providing access to the portal to third parties.
    e. Applications for registration of patients under 16 years of age should be reviewed on a case by case basis and a tiered approach to parent/guardian access should be adopted.
    f. Privacy officers in participating general practices to be ready for correction requests.
    g. Further privacy impact assessment to be obtained if it is proposed the information is to be used for another purpose.

Dated at Christchurch this 5th day of November 2015

G F Abdinor

Taylor Shaw

A. Introduction and Overview

Introduction and Overview

1. This Privacy Impact Assessment (PIA) has been commissioned by Compass Health.
2. Compass Health is a Primary Health Organisation (PHO) that provides a wide range of primary care services through 60 general practice teams and a number of other health care providers throughout the Wellington, Porirua, Kapiti and Wairarapa regions.
3. Compass Health Wellington Trust (previously named the Greater Wellington Health Trust) was formed in 1997 to contract with District Health Boards and other funders to provide health services, and was managed by the Wellington Independent Practitioner's Association (WIPA, formed in 1995). Compass Health in its present state was formed in July 2010 by the merger of three existing PHOs: Capital PHO, Tumai Mo Te Iwi, and Kapiti PHO. Wairarapa PHO was then merged into Compass Health in 2012.
4. Compass Health is the licence holder of the ManageMyHealth™ software on behalf of other Primary Health Organisations (PHO) in the Central Region including; Central PHO, Well Health Trust, Ora Toa Health Services, Cosine, Te Awakairangi, Whanganui Regional Health Network and Health Hawke's Bay.
5. Compass Health has contracts with health professionals and organisations in the community such as General Practitioners and the wider general practice teams, to help deliver quality health services to their patients.
6. This Privacy Impact Assessment (PIA) will outline a recommended implementation approach which will be adopted by Compass Health and could be adopted across the other Central Region PHO Networks.
7. The introduction of patient portals contributes to Compass Health's long term goals of '*improving the patient experience of care*' and '*strengthening general practice capability*'. Through enabling practices to implement the portal, primary healthcare delivery will be enhanced, changing the way care is delivered and enabling patients to take more control of their own care.
8. The ManageMyHealth™ patient portal has already been implemented in several areas and is now at the stage of implementing a wider rollout of the patient portal across the Central Region.

Introduction to Patient Portals

9. A patient portal is a website that gives patients online access to their own personal health information / patient health record to enable the patient to manage aspects of their own healthcare.
10. A patient portal potentially allows patients to access:
    a. Notes from a health care consultation;
    b. Diagnosis;
    c. Medical conditions;
    d. Discharge summaries;
    e. Medications;
    f. Immunisations and vaccinations;
    g. Screening information;
    h. Laboratory / Medical imaging results, including annotations (if any).

11. Patient portals also generally include the ability to request repeat prescriptions, book appointments, send and receive secure messages, set reminders and recalls and manage health goals.

12. Definitions of patient portals invariably include the word "secure" as security of the information is an essential aspect of a patient portal. The security of the patient portal cannot however be assumed for the purpose of a Privacy Impact Assessment and the security must therefore be evident.

13. The New Zealand National Health IT Board supports the implementation of patient portals by general practices.[1] Implementation is also supported internationally as many health service providers, including publically funded providers, recognise the benefit of patients actively engaging in their health and welfare through access to their health information.[2]

14. Identifiable benefits of a patient portal include:

    a. Visibility of health care services for patients;

    b. Better opportunity for patients to understand their health/well-being and to engage in treatment and care;

    c. Improved safety as patients can refer to the record in engaging with other health care providers such as an emergency department;

    d. Patient can raise issues with healthcare providers such as delays in test results or referrals

    e. Better management of on-going conditions;

    f. More efficient use of time in treatment and care: for example less need for explanations and review, 'telephone tag' for appointments; managing repeat prescriptions and recalls; and

    g. Reduction in paperwork.

15. However, there are privacy concerns and issues to be addressed. As noted above, security is critical to a patient portal. If the agency implementing the portal is not able to provide the technical security necessary, either through ability or resource, then there is a risk to privacy as well as the relationship of trust and confidence between the healthcare provider and the patient.

16. The risk is real. On 4 February 2015, Anthem, a large private health insurer in the United States, announced it had been the subject of a sophisticated cyber-attack which left 80 million health records exposed.[3] Combining health records in one location creates a target for these sorts of attacks.

17. There are other privacy issues:

    a. Governance: ensuring the patient portal has the right governance structure in place to ensure proper delivery of the patient portal including functionality, ongoing quality improvement and education, auditing, legal compliance and privacy enhancing processes.

    b. Source of data: has the patient authorised collection from all sources of data?

---

1 http://ithealthboard.health.nz/patient-portals

2 http://www.england.nhs.uk/ourwork/pe/patient-online/; http://www.healthit.gov/providers-professionals/faqs/what-patient-portal
http://www.ehealth.gov.au/internet/ehealth/publishing.nsf/content/home; http://mypatientaccess.ca/

3 http://www.forbes.com/sites/danmunro/2015/02/05/health-data-breach-at-anthem-is-a-blockbuster-could-affect-80-million/

The patient does not have to authorise collection of personal information from all sources under the Health Information Privacy Code. When authorisation is not required the reason why should be recorded on the patient's file to refer to in the case of a complaint.

c. Patient login protocols/authentication: ensuring the patient is the person accessing their own health information through clear identification and secure passwords.

d. Abuse: the risk that patients are forced to give access to their health information to other people such as employers or family members under duress. While arguably this is the patient's responsibility to ensure they do not give access, either through logging on themselves and leaving the open portal to another party to view or revealing their log-on password, it is known to the health industry that there are oppressive relationships where vulnerable patients may feel obliged to provide access. This can include children and elderly.

e. Identity theft: through cyber breach of security or inadvertent disclosure of access.

f. Correction requests: agencies need to be prepared to deal with correction of health information and challenges to accuracy as a result of increased patient access. There are strict time limits that must be complied with and resources need to be allocated to deal with such requests.

g. Confidential information: agencies need to be ready to deal with information they can legitimately withhold from patients, such as information which will involve the unwarranted disclosure of a third party's affairs or information which could lead to serious harm to the individual or to others.

h. Functional creep: the patient portal will contain the health records of numerous patients creating an information hub which will be of commercial interest to some agencies and of legal interest to other agencies such as the police, immigration and the courts. While the information requests from such agencies may be for good reasons, the existence of the database and the ease of access by portal providers may impact on patient's desire to provide full information for their treatment and care in the fear of risk of disclosure.

i. Unauthorised staff access to health records: this is an issue for healthcare providers generally in the use of electronic records but also an issue for the IT agency providing the portal. Access levels for these 'privileged users' need to be identified, as well as appropriate authorisation and controls.

18. Without minimising the benefits of patient portals, the privacy risks, especially in security, are real and significant. It is important that any patient portal operates in a highly secure environment with privacy enhancing responses built into the system.

19. Compass Health has used the label 'Health Care Online' for the purpose of familiarising the concept of a patient portal to General Practices and patients.

Introduction to Privacy Impact Assessments

20. A PIA[4] is a systematic process for evaluating a proposal in terms of its impact upon privacy. It is designed to identify the potential effects that a proposal may have on an individual's privacy, examine how any detrimental effects upon privacy might be

[4] Privacy Impact Assessment Handbook, Office of the Privacy Commissioner 2007: https://www.privacy.org.nz/news-and-publications/guidance-resources/privacy-impact-assessment-handbook/

overcome and ensure compliance with the health information privacy rules set out in the Health Information Privacy Code 1994.[5]

21. Elements of a PIA include an introduction and overview, description of the project and information flows, the privacy analysis, privacy risk assessment, privacy enhancing responses, compliance mechanisms and conclusions. This assessment is prepared with reference to the guidelines issued by Office of the Privacy Commissioner.

22. There are obvious privacy issues which arise from any patient portal as identified above. There are also general privacy and confidentiality issues which immediately arise from any proposal which involves a health information record as:

    a. health information is sensitive and must be protected;

    b. health information is collected in a professional relationship of confidence and trust and there must be no risk to that relationship;

    c. health records must be accurate; and

    d. it is important to comply with obligations under the Health Information Privacy Code 1994, the Public Records Act 2005, and the Code of Health and Disability Services Consumers' Rights together with relevant standards such as the Health and Disability Services Standards (NZS 8134: 2008), the Health Records Standards (NZS 8153: 2002) and the Referrals, Status and Discharges (RSD) Standards: Business Process (HISO 10011.1), Messaging Standard (HISO 10011.2) and Implementation Guide (HISO 10011.3). There are Codes of Practice and Protocols such as the Health Network Code of Practice (SNZ HB 8169:2002) and the Ethnicity Data Protocols for the Health & Disability Sector 2004.[6]

23. Patients and health service providers need to have trust and confidence that the system is legally compliant, meets professional obligations of confidentiality and privacy and does not provide unnecessary and unauthorised access to patient health information.

24. This PIA has involved reference to the specifications for the system and has been prepared in consultation with representatives of Medtech Global Limited and Compass Health.

25. A draft of this assessment report has been circulated to the Office of the Privacy Commissioner for feedback. That feedback has been incorporated into this Assessment.

[5] The Health Information privacy Code 1994 is a code of practice issued by the Privacy Commissioner under the Privacy Act 1993. See: https://www.privacy.org.nz/the-privacy-act-and-codes/codes-of-practice/health-information-privacy-code/

[6] The National Health IT Board has helpfully identified, approved and endorsed relevant standards which can be viewed through its website: http://ithealthboard.health.nz/standards.

B. Description of the project and information flows

Patient Portal

26. Compass Health and the other Central Region PHOs are looking to support general practices to implement a patient portal into general practices across the Central Region.

27. There are multiple patient portal products on the market; however this Privacy Impact Assessment will discuss the implementation of the Medtech Limited ("Medtech") ManageMyHealth™ platform. Medtech Limited is independently accredited for ISO 9001 Quality Management Systems and also independently certified for Information Security Management System (ISMS: ISO 27001)

28. The ManageMyHealth™ website (http://managemyhealth.co.nz/) includes a comprehensive privacy statement which is annexed to this document as Schedule 1.

29. Compass Health has also created a comprehensive setup guide for general practices. This guide is called *Health Care Online: Start-up Guide for General Practice* ("the start-up guide"). The start-up guide contains example resources including a patient brochure, template consent form, example terms and conditions and a guide for reception use.

30. Implementation of a patient portal by general practices is on an opt-in basis and each participating general practice will be responsible for selecting which of their patients are provided access to the portal and various key clinical and business decisions relating to the information available to each patient via the portal and the services offered via the patient portal to their patients.

31. These key decisions include but are not limited to:

    a. Which patients will be provided access to the portal (will access be provided to selected patients or universally across the practice);

    b. The fees (if any) that will be charged for certain services provided through the patient portal;

    c. Which providers within a practice will receive secure messages from the patients;

    d. How quickly these messages will be responded to;

    e. What optional health information will be made available to the patients through the patient portal; and

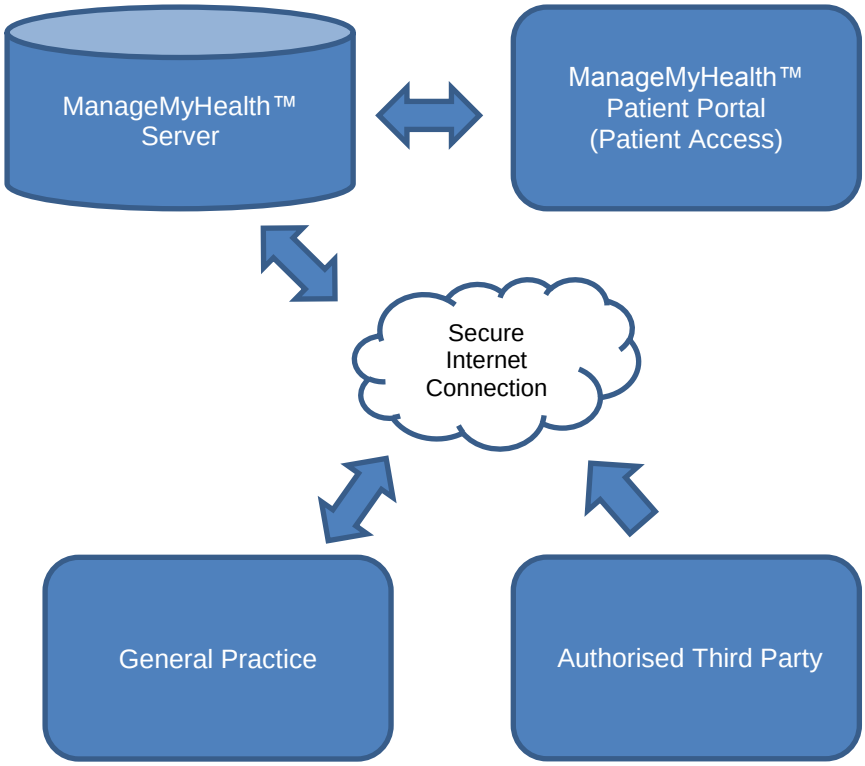
    f. How laboratory results will be dealt with in the patient portal.

32. There will be two types of information accessible in the patient portal:

    a. Information sourced from the patient's general practice; and

    b. Information uploaded to the portal by the patient or third parties authorised by the patient.

33. The diagram below illustrates the information flows:



Data

34. The health information that could potentially be made available through the portal is significant and includes:

    a. Basic patient details such as full name, gender, address, date of birth, national health index number (NHI), phone number, cell phone number, email address, emergency contact person and any additional demographics (eg ethnicity);

    b. Prescriptions;

    c. Allergies;

    d. Immunisations;

    e. Diagnoses;

    f. Laboratory results;

    g. Consultation notes;

    h. Recalls

    i. Measurements; and

    j. Names of relevant health care providers associated to each health record item.

35. The information can be characterised at the general practice as sensitive and highly confidential.

36. As noted above, each general practice is able to determine the types of information available via the patient portal.

37. It is possible to withhold certain items from the patient record so that the items are not available via the portal. Items that can be withheld from the portal include but are not restricted to diagnosis, medications and inbox items.

Who will be able to access information via the patient portal?

38. Each participating general practice will determine which staff members and patients will have access to the patient portal. Each staff member and patient offered access to the patient portal will need to register. Registrations will be linked to the individual's unique email address.

39. Each patient will be required to provide a unique email address as part of the registration process. This should be a personal email address which is not shared with another person. This address also should not be used for any other person to register to the Patient Portal.

40. Each patient will be identified by the general practice by:

    a. enrolment process to the practice or

    b. photo identification or

    c. clinician endorsement

41. Each patient will also be required to complete a patient consent form as part of the registration process.

42. The ManageMyHealth™ website provides that parents can register their children as users of the patient portal, so that the parents can access their child's medical records. Compass Health has recommended that registration applications for patients under the age of 18 years of age should be reviewed on a case by case basis. Each participating general practice should consider their own restrictions in regards to patients younger than 18 years of age and should consider a process which reviews access at different ages. The privacy implications of this will be discussed in more detail in the next section of this assessment.

43. Compass Health recommends the following access parameters are implemented for patients under 18:

    a. Patients under the age of 10 years can register to use the portal and the primary parent/guardian of the child should be responsible for maintaining control of their account.

    b. Patients between 10 years and 15 years old can register to use the portal and their accounts should be flagged to providers so that they're aware that the parent/guardian may have access to the child's portal and should treat information sensitively as appropriate.

    c. Patients 16 years old and older can register for their own accounts with no parental access provided.

    d. Where patients under the age of 16 are registering to use the portal, the patient's parents/guardians should complete a separate registration form which outlines the special access provisions for these patients – namely that parent/guardian access to the portal may be removed at the request of the child, if conflict between parents/guardians arises and/or when the child turns 16.

44. There is potential for patients to provide access to their records in the portal to trusted third parties (for example, family members) in the future.

45. The level of access for staff members will be at one of three levels: administration ("Admin"), Reception or Clinical. The *Admin* permission level allows the staff member to alter administrative configuration and is recommended for the practice manager. The *Reception* permission level allows the staff member to view basic demographic information about the patient and allows them to register a patient for the portal. The *Clinical* permission level allows the staff member to view the clinical detail within the

system and it is recommended that this access level is only provided to doctors and registered nurses in the practice.

46. When a staff member or patient leaves the practice, it is recommended in the start-up guide that their access to the portal should be removed by the practice.

47. Usage reports and statistics are available through the portal and can be used by the general practice to audit access and usage of the portal. Likewise, the comprehensive access log or history can be used by the patient to audit access to their information.

How is access provided?

48. Access is provided to both patients and providers via a secure website protected by firewall and accessed using an encrypted password.

49. Access is also available via iOS App from the App Store and Android App from Google Play. Both Apps access the secure website protected by firewall require the use of the same encrypted password used for the secure website. No data is stored on the mobile devices

The Agencies involved in Patient Portal

50. As identified above, key agencies are Compass Health, the other Central Region PHOs, Medtech and the individual general practices.

51. Compass Health's Patient Portal Operational Team will be the operational resource that is used on a daily basis to support the participating general practices to implement the Patient Portal.

52. This team will be overseen by the Information Management Service Level Alliance (IMSLA) Governance Group, which governs a range of ICT initiatives, including the Shared Care Record project and patient portals, for the Capital and Coast, Hutt Valley and Wairarapa District Health Board regions. The IMSLA will:

    a. provide project data governance;

    b. policy and procedure oversight;

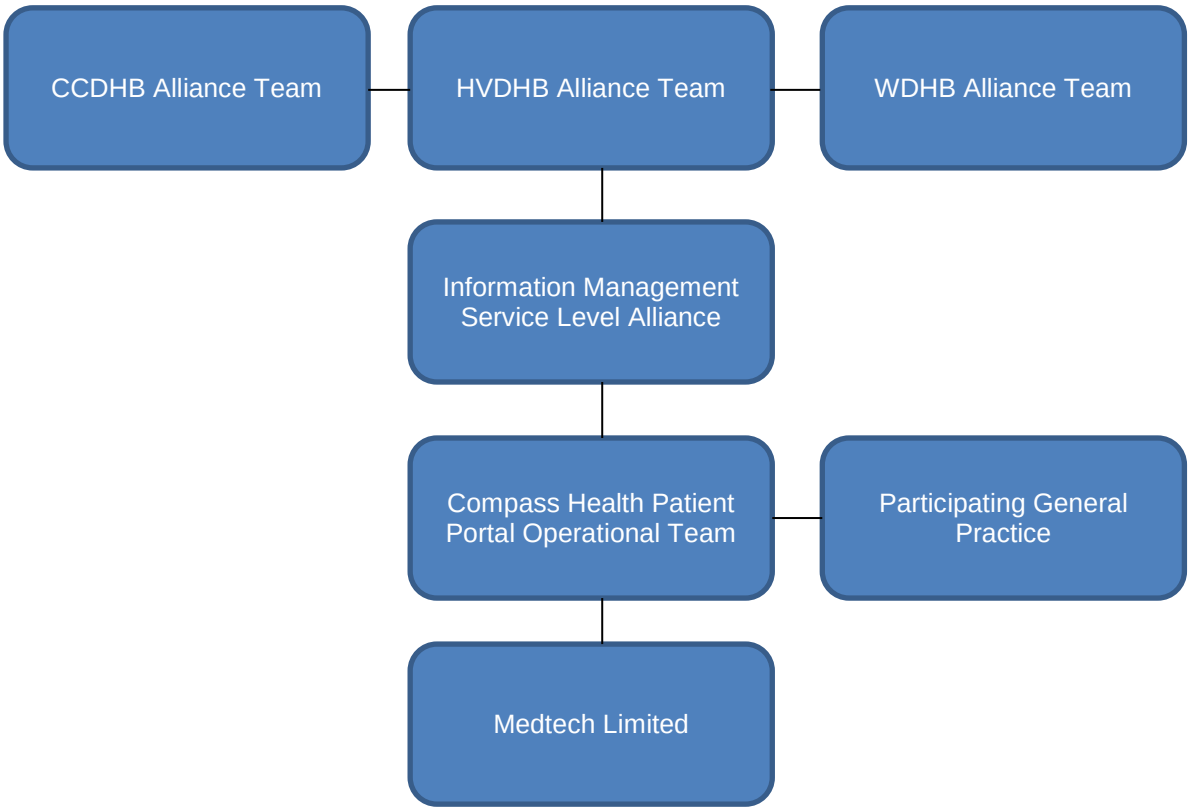
    c. appointment of clinical auditors where necessary;

    d. review privacy audits and outcomes; and

    e. be responsible for approval and control of any significant changes or expansions to inter-organisational information sharing projects.

53. The IMSLA governance group reports to the alliance leadership teams of the Capital and Coast, Hutt Valley and Wairarapa District Health Boards and it will continue to monitor the patient portal project as required during and post implementation.

54. The diagram below illustrates the governance structure for the project:



C. The Privacy Analysis

Introduction

55. The Health Information Privacy Code 1994 provides guidelines on the collection of health information (rules 1-4). Health information should only be collected for the necessary and lawful purposes of the agency, health information should be collected from the patient concerned unless an exception applies, health agencies should be transparent about collection of health information, how it is to be used and by whom, and collection should be lawful and fair.

56. Guidelines on security (rule 5), access and correction (rules 6 & 7), accuracy (rule 8), retention (rule 9), use and disclosure (rules 10 and 11) and unique identifiers (rule 12) are also provided.

Collecting or Obtaining Information

57. Health Information must be collected for the necessary and lawful purposes of the agency (Rule 1). In this case, some of the health information has already been collected from the patient by the general practice for the provision of health care services. All that is proposed is that the patient be able to view some of that data.

58. Other health information will be uploaded to the patient portal by the individual (or potentially in the future by third parties authorised by that individual) for the purpose of documenting health goals and recording progress in achieving them.

59. The purposes are lawful and necessary. As healthcare moves into more active participation from patients, patients need access to their data. Having said that, participation is not compulsory – patients are not required to agree to use of a patient portal as part of the provision of health services.

60. As with any collection of health information, under rule 3 there must be transparency. Patients need to know the purposes of collection and, importantly who may see it. Patients will need to know about the relevant agencies, including Medtech, who as a platform provider will have access to data.

61. Rule 4 says information should not be collected by unfair means. In this case, as participation in the patient portal is voluntary, there is no issue with rule 4.

Security

62. Security must be addressed in order to comply with Rule 5 of the Health Information Privacy Code 1994, the Health Network Code of Practice and the RSD Standards.

63. Rule 5 requires a health agency which holds health information to ensure that the information is protected by such security safeguards as is reasonable in the circumstances to take against:

    a. loss;

    b. access, use, modification or disclosure without authority; and

    c. other misuse.

64. While agencies are only required to take reasonable security measures, the high level of confidentiality and sensitivity of the information requires on-going vigilance due to the risk of new and sophisticated cyber attacks. Staff need to be continually training and familiarising themselves with the risk and implementing appropriate protections as well as monitoring the system. The recent cyber attack on Anthem, as described above, was not discovered for a two week period.

65. Rule 5 also requires a health agency to dispose of documents in a matter which preserves privacy and to ensure that if information is given to a third party that

anything reasonably within its power is done to prevent the unauthorised use of disclosure of that information.

66. In terms of security, key issues arising from the patient portal are:

    a. Authentication;

    b. Transmission;

    c. Firewall security and cyber attacks;

    d. Backups; and

    e. Access to the data.

67. The first 4 issues of these relate to the security of the technology used in the system and the last issue primarily relates to the users of the system.

Operational Security (Technology)

Authentication

68. Given the sensitivity of health information, it is critical that users accessing the patient portal are properly authenticated – that is, they are who they say they are.

69. Patients are required to be identified by the general practice and provide a unique e-mail address when registering for the patient portal, and to set up a password to be used to authenticate their identity when accessing the portal. The password requirements include a minimum of 6 characters and a mix of alpha numeric characters.

70. The use of passwords for authentication, especially for sensitive information like health information, has increasingly become the subject of criticism, especially given the password conundrum – short and simple passwords are easy to remember, but they are also easy to guess or hack. Long and complex passwords are more difficult to guess or hack but difficult to remember, often resulting in password re-use, which increases vulnerability if the password is compromised.[7]

71. Responses to this challenge include the use of two factor or two channel authentication. An example of two factor authentication is where a password is used in conjunction with a unique code sent to the user's cell-phone or in conjunction with a fingerprint or retinal scan. The use of two factor or two channel authentication is however perceived as being less convenient for the user.

72. Another risk with the use of passwords for authentication is brute force attacks, which is where automated software is used to generate a large number of consecutive guesses of what the password might be. To provide protection against these types of attacks a user account is blocked after 5 failed log-on attempts.

Transmission

73. Transmission of data (including for secure messaging between the patient and practice) is managed through encryption and HTTPS, which is a well-recognised secure internet protocol. Data is encrypted using 256 bit encryption where the patient uses the latest browser versions and 128 bit encryption where older browser versions are used.

74. Messages sent through the portal between the patient and the practice do not leave the ManageMyHealth system and thus remain protected by the transmission safeguards, unlike regular email messages.

[7] *Should the FTC Kill the Password? The Case for Better Authentication* by Daniel Solove and Woodrow Hartzog, Privacy & Security Law Report, 14 PVLR 1353, 07/27/2015

75. ManageMyHealth™ New Zealand is hosted in a secure commercial data centre in New Zealand. No data is stored by ManageMyHealth™ outside of New Zealand."

Firewall

76. ManageMyHealth makes use of an industry standard server firewall to protect against cyber attacks.

Destruction

77. The health information uploaded to the portal is not deleted unless the user's access to the portal is terminated. There will need to be direction about this in accordance with the Public Records Act 2005 (if applicable), the Health (Retention of Health Information) Regulations 1996 and rule 9 which requires health information to be held only for as long as necessary.

Printing

The Patient Portal does not allow for the entire health record to be printed via the ManageMyHealth™ application. This is an additional security provision to minimise the risk of health information being easily extracted from the safety of the portal environment and then used for other purposes. The ManageMyHealth™ application policy to supporting printing is to enable only ability to print in specific scenarios. (e.g. ManageMyHealth™ provides for Test results to be printed as users have requested this capability.)*Operational Security (Users)*

78. Systems also need to be in place to ensure that there is a proper authority matrix for access to the patient portal and its data by staff from the participating general practices. There should be appropriate consequences for staff implementing the system accessing data inappropriately. Depending on the behaviour involved, this should include an enquiry process with the ability to refer the matter to an individual's employer or professional body (if necessary). There should also be the ability to lock out or refuse access to the system to any staff member.

79. Compass Health already has contractual arrangements in place to ensure that information available to Medtech is not to be used for any other purpose other than serving information to authorised users (providers or patients). The only exception to this is where the information is properly anonymised or de-identified so that it can be used for marketing Medtech's product. The patients need to be educated and made aware of the risk of sharing their passwords with anyone or being pressured into providing access to their records via the portal. Patients should be made aware that they can contact the general practice if they have any concerns about being pressured to provide access to their health information.

Access and correction

80. Rules 6 and 7 gives individuals the right to ask an agency if it holds health information about him or her and, in most cases, to have access to that information. That person has also the right to request correction of any of the information held about him or her.

81. The whole point of a patient portal is to provide automatic access to registered patients, so the main issue will be ensuring there is resource in place to deal with rule 7 requests in respect of correction. International experience suggests that these requests rise significantly once patients have access to their information.

82. The ManageMyHealth privacy statement does provide that Medtech will act reasonably to ensure users will have access to their information at anytime, except in certain stated circumstances which include where ManageMyHealth requires a planned outage. Compass Health should obtain further information from Medtech

regarding these planned outages so that users can be told up front what reasonable availability to the portal will be.

83. Each participating general practice also needs to be ready to deal with information they can legitimately withhold from patients, such as information which will involve the unwarranted disclosure of a third party's affairs or information which could lead to serious harm to the individual or to others.

84. Accordingly, each participating general practice will need to ensure its privacy officer is prepared for such requests which will likely require additional resource in support.

85. As noted above, Compass Health believes that there are medical benefits to patients under the age of 16 having access to the patient portal and recommends that a tiered approach is adopted to manage the potential privacy concerns that may arise from this access. Compass Health recommends that applications for registration for patients younger than 16 years of age be reviewed on a case by case basis by the general practice. Given that parents/guardians do not have an automatic right of access to their children's information, this is a sensible safeguard to manage the risks inherent in providing them with 'automatic access' to their child's health records via the patient portal.[8]

86. Additionally, Compass Health recommends a tiered approach to parent/guardian access to their child's portal:

    a. where the patient is under 10 years old the primary parent/guardian is provided access to the child's portal;

    b. where the patient is 10 to 15 years old the patient's record if flagged to highlight that the parent/guardian may have access to the portal and information should be treated with appropriate sensitivity; and finally

    c. where the patient is 16 years old no parent/guardian access is provided.[9]

    This tiered approach can be tailored as appropriate by the general practice.

87. Compass Health also recommends that parents/guardians being provided access to their child's portal should be required to complete a supplementary registration form which confirms their identity, legal relationship with the patient and that access to the portal may be removed at the patient's request, where conflict arises between parents/guardians (due to the potential disclosure of personal information about one parent to another), and/or where the patient reaches 16 years of age. This appears to be a sensible approach to managing the potential privacy risks that may arise from parent/guardian access to a child's patient portal.

Accuracy

88. Rule 8 requires a health agency to take reasonable steps to check accuracy of information before use.

89. The relevance of rule 8 is that it flows on from rule 7. If a patient identifies incorrect information and seeks to have it corrected, this can create an issue for the participating general practice if it seeks to rely on incorrect data. Correction requests are relevant to rule 8.

90. Additionally, patients are able to upload their own health information to the patient portal.

91. All health information is labelled with the source of the information.

[8] Refer Rule 11 of Health Information Privacy Code and section 22F of the Health Act 1956

[9] The ages in the respective tiers were chosen to align with Youth Medical Services which are available to patients from the age of 10 years. The tiers are only a guideline however and will need to be reviewed on a case by case basis.

92. Patients are currently able to upload the following information to the patient portal and make this available to the general practice (or keep as personal record).

    1. Demographic details;

    2. Measurements (weight, blood pressure etc.);

    3. "Journal" entries;

    4. Goals and Tasks; and

    5. Attachments to messages.

93. The demographic details will be sent to the practice automatically to enable the practice to confirm if it would like to update its system with the new information.

94. The practice can choose which measurements should be imported into the practice system if added by the patient. The practice then has the opportunity to review the measurement before 'filing' or adding to the practice system.

95. "Journal" entries, goals and tasks are promoted as 'personal' tools. The patient can share these entries with the General Practice however the message stays on ManageMyHealth and is not saved in or sent to the practice system.

96. With attachments to messages (similar to the usual e-mail attachment function) the message will be stored within the patient record in practice system. The practice can set terms and conditions to be accepted before sending this type of messaging.

97. Care needs to be taken to check the accuracy of any patient provided information before it is relied upon by the General Practice.

Use and disclosure of information

98. Rule 10 requires a health agency to use information for the purposes for which it was collected. The health data was collected in order to provide health services to patients. It is now proposed to share that data in one system to enable patient access at a single point of contact (the patient portal). This requires consent.

99. Rule 11 states that health information should not be disclosed to third parties unless an exception applies which includes consent. The patient portal requires the general practice to share data with Medtech, as the platform provider, and that should be with patient consent.

100. ManageMyHealth's Privacy Statement also provides that "Medtech may disclose personal information if required to do so to … protect and defend the rights or property of Medtech and our family of websites". This use and disclosure requires consent.

Unique Identifiers

101. Rule 12 of the Health Information Privacy Code 1994 does not allow a health agency to assign a unique identifier unless it is necessary to the agency's functions. Though health agencies are not to use unique identifiers assigned by another agency, the use of the National Health Index (NHI) number is permitted throughout the health sector. Unique identifiers should not be assigned until a person is properly authenticated.

102. In this system there are a number of unique identifiers: the NHI and authentication identifiers. It appears the use of these unique identifiers is compliant with Rule 12.

D. Privacy risk assessment and Privacy Enhancing Responses

103. This section summarises the key points identified above and provides a list of issues and/or responses.

104. There needs to be clear governance of the patient portal with proper management flowing from that governance.

105. Governance involves ensuring there are systems in place to ensure integrity and security. In implementing the patient portal there should be clear processes for ongoing quality improvement and education, auditing, legal compliance and privacy enhancing processes.

106. The governance group should require Medtech to notify the governance group's administrator and all ManageMyHealth™ users if any changes are made to the ManageMyHealth™ Privacy Statement.

107. In particular, Compass Health and each participating general practice needs to be careful that the single point of access and sharing of health data (creating an information hub) does not lead to functional creep and turns the database into a repository of information for commercial interests or for the police/courts. Third party access requests should be managed as they are currently with existing health records.

108. The agencies involved need to have clear agreements between them as to their individual obligations/responsibilities to ensure privacy and confidentiality is maintained in transmission of data and access. Each participating general practice and Medtech will need to ensure information transmitted from their systems is encrypted and sent safely into the patient portal. Medtech needs to ensure information received and information accessed is stored securely and transmitted securely.

109. Each participating general practice will need to consider if there is any data which needs to remain confidential and which could be legitimately withheld from patients, such as information which may involve the unwarranted disclosure of a third party's affairs or information which could lead to serious harm to the individual or to others.

110. The participating general practices will need to consider whether they will allow patients under the age of 16 to register as users of the patient portal and whether parents will be allowed to register their children as users. Compass Health has recommended that applications for patients be reviewed on a case by case basis and where appropriate a tiered approach to parent/guardian access, based upon the age of the patient, be adopted, along with supplementary registration by the parent/guardian that is provided access to their child's portal. This supplementary registration form should make it very clear that parent/guardian access to their child's health information via the portal can be reviewed and potentially removed at any time and at the patient's request, where the practitioner believes appropriate and where the patient reaches 16 years of age. This seems like a sensible way to manage the privacy risks inherent in providing 'automatic access' to health information to children and/or to their parents.

111. The participating general practices and Medtech need ongoing vigilance against operational security risks, including ongoing staff training, system monitoring and auditing of access and use of the portal.

112. Medtech and each participating general practice will need to ensure that they have the following in place:

    a. A privacy policy including clear policy guidelines on the use of the system together with training;

b. Staff confidentiality agreements;

c. Access matrix identifying roles and access restrictions;

d. Authorisation controls defining which staff of which agencies may add, or correct information on records and electronic foot printing of user access;

e. Process for destruction/removal of health records in compliance with the law;

f. Managing and reporting of privacy breaches (Office of the Privacy Commissioner guidelines recommended);[10]

g. A complaints process for patients who are concerned with their health information management; and

h. The role of a Privacy Officer. The privacy officer will not only need to be alert to patient requests for correction to records but also requests from other agencies such as the Police, Courts, government agencies and insurance companies. The response to these requests should be consistent with law and established policies.

113. Each participating general practice will also need to be prepared for correction requests as patients' access the portal.

114. There needs to be good information, including a privacy statement, available by pamphlet and on a website, explaining to patients how the patient portal works, how information is gathered into a single source and from where, how the information may be used and disclosed, who has access to it and who the agencies involved are. Patients should also be told what percentage of the time the service, taking into account planned outages, will be available to them. A help desk is also recommended.

115. Patient login/authentication must be secure enough to avoid identification theft. Patients need to know about keeping their login secure and their ability to let their healthcare provider know if anyone is putting pressure on them for inappropriate access to their data.

116. Enrolment for access to a patient portal will need to show patient consent and understanding of the above matters.

[10] The Office of the Privacy Commissioner has developed privacy breach guidelines which are recommended: see *Key Steps for Agencies in Responding to Privacy Breaches and Privacy Breach Checklist* : www.privacy.org.nz

G. Conclusions

117. The implementation of patient portals fits well with Compass Health's long term goals of improving the patient experience of care and strengthening general practice capability. There is the potential for portals to assist patients to engage with their own health management and to enable primary health resources to be used more efficiently and effectively.

118. Care will however need to be taken to address the potential privacy risks that arise from the use of patient portals to ensure that the relationship of trust and confidence between the patient and general practice is not put at risk.

Schedule 1 – ManageMyHealth Privacy Statement

ManageMyHealth™

Privacy Statement

Last Updated on Friday, January 1, 2010

Introduction

Medtech Limited is committed to protecting your privacy through its secure 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.

Part A – General Privacy Statement

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.

Storage of information

Any information or records you maintain with a ManageMyHealth™ account will be hosted on servers in a secure 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.

Security

When any information is uploaded to your ManageMyHealth™ account, it sends it over the Internet using Secure 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 secure 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.

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™.

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.

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.

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.

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.

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.

Use of cookies

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

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.

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

or

Email: privacy@managemyhealth.co.nz

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.

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.

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.

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.

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 eg. 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.

Rule 5 Storage and Security of Health Information

Storage of information is hosted in a secure 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.

Rule 6 Access to Personal Health Information

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

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.

Initially access to your information will be limited to you and the registering Healthcare Provider eg. your doctor, including other clinicians within your Healthcare Provider Practice. This will be expanded in later versions to allow other healthcare professionals you authorise and an optional "trust list" functionality which will allow you to grant access to other individuals involved with your care, such as your family members.

Rule 7 Correction of Health Information

Information entered by you can be modified at anytime.

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.

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.

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.

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.

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.

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.