Electronic Shared Care Records

Elements of Trust

SEPTEMBER 2014

Privacy Commissioner
Te Mana Matapono Matatapu

Privacy Commissioner
Te Mana Matapono Matatapu

Contents

Executive Summary

Shared Care Records (SCRs) are a tool for allowing wider access to health information by health professionals for the purpose of care. In an increasingly electronic health environment SCRs can facilitate care and enhance privacy by increasing clinician access to, and patient control over, health information.[1] SCRs have the potential to be accessed directly by the patient[2] and health care providers, and both authorised and unauthorised access can be accurately tracked.

However SCRs carry an increased risk of unauthorised access because they are open to a much greater number of people. As an extensive collection of accurate and well-ordered information they are also susceptible to function creep, where information collected for one purpose is used for another. If patients and health providers (such as GPs) become unsure that health information is being properly protected, they will be unlikely to support the introduction and continued use of SCRs.

This document reviews three existing regional SCRs:

1. Care Insight in the Northern region
2. Compass Health in the Central region
3. eSCRV in the Southern region

This review identifies common elements, shared solutions, and how any potential privacy issues have been identified and mitigated. It also makes recommendations about which elements of these and other SCRs should be considered compulsory from a privacy viewpoint.

Our initial findings are that the three SCRs are well-managed projects that have accomplished their clinical goals while appropriately mitigating privacy risks and complying with their obligations under the HIPC.

However ongoing attention needs to be given to:

- **transparency** (to ensure patients are aware of how their information is being shared)
- **governance** (to preserve the security of the health information held and prevent function creep), and to
- **security** (to foster and maintain adherence to the Health Information Security Framework).

[1] A useful summary of the potential benefits can be found at http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1949437/

[2] For the purpose of this paper, 'patient' includes all health consumers, whether well or unwell

More broadly, SCRs would benefit from operating in a manner which does not presume a high level of consumer and clinician trust in the integrity of health sector information handling practices.

Common elements of the SCRs

Of the three systems, two do not seek individual patient consent for information to be stored on the system. However, all three systems require patient consent, where practicable, before health practitioner's access information. Some other common elements of the three SCRs are:

- Online summary care record based on GPs' computerised Practice Management System (PMS)
- Public notification of existence of system by way of posters and pamphlets in GPs offices
- Easy access to opt-out facility for patients
- Summary of health data online via secure network, with potential for addition of more detailed information at a later date
- Access by authorised health professionals via password/login with permission, or as needed to provide care where permission is not available
- No intentional provision for secondary purposes beyond health care
- Eventual provision for patient access to their own information via password/login
- Recording of all data access and alteration ("footprinting")
- Manual and automated scrutiny of data access
- Consequences for individuals who misuse the system, extending beyond removal of access privileges

Notes on legal status of health information held on SCRs

- Health professionals accessing an SCR are considered to be collecting information from a source other than the patient and therefore need either the patient's permission or another good reason to do so under rule 2 of the HIPC (for instance where the patient is unavailable or unable to give consent)
- Responsibility for the security of the collection as a whole rests with the agency operating the SCR
- Responsibility for the security of any health information collected from an SCR rests with the agency that collected it

Recommendations

Health care occurs in an environment that demands a high level of trust. Patients need to trust their care providers; care providers need to trust that other providers will properly manage the information that is entrusted to them. Trust takes time to build, but can be damaged in a very short space of time. Two of the key elements that foster and support trust are **control** and **transparency** in the context of an ongoing relationship. Health information also requires proper **governance** and appropriate **security standards**.

CONTROL

- **SCRs should allow patients and clinicians to easily opt out if they wish.**
  - For instance: 0800 free phone line, or via GP.
  - Consequences of opting-off (e.g. that certain kinds of care may be made more difficult or that the patient may be put at increased risk) should be stated in a clear but not alarmist way.

- **Secondary purposes should be minimal and tightly regulated to help maintain clinician and consumer trust.**
  - SCRs hold information on behalf of the clinicians who provided the information and the primary purpose is always to provide high quality care to patients.
  - Secondary purposes such as service improvements, teaching, research and audit must be well-publicised and use anonymised or pseudonymised data wherever possible.
  - Any new secondary purposes should only be adopted with proper consultation and with careful consideration of the potential risk to public trust in the SCR.

- **Users of the SCR should only access the record with patient permission, unless a justification exists for doing so under rule 2 of the HIPC.**
  - Repeatedly obtaining permission is not necessary, nor is obtaining permission where not reasonably practicable or where it would prejudice the interests or safety of the patient.
  - A 'tick box' screen requiring users to confirm that they either have patient permission or another justification exists for accessing the SCR is an appropriate protection.

- **All data access and use should be recorded and retained.**
  - Automatic recording of information about every access to an SCR ('footprinting') is an important safeguard against misuse.
  - While standards for retention of footprint information are still being developed, retention for a minimum of two years is a reasonable expectation.

TRANSPARENCY

- **Agencies operating the SCR must provide resources that make it as easy as possible for participating agencies (e.g. GPs, hospitals, testing laboratories) to publicise the existence of the SCR and the parameters around its use.**
  - At a minimum this would include brochures and posters in GP waiting rooms and a website with clear Plain English explanations of the SCR.
  - Training for staff is also vital, in conjunction with an overall culture of privacy, to ensure that patient questions can be answered and concerns addressed

- **Primary health care providers such as GPs that are using SCRs should take reasonable steps to notify their patients about the existence of the SCR and the parameters around its use**
  - For instance keeping stocks of brochures updated, posters prominently displayed, and conducting low-cost population notification by email or adding an explanatory brochure when sending mail to patients

- **Agencies operating the SCR should publish their privacy analysis underpinning the privacy safeguards of the SCR.**

GOVERNANCE

- **There must be a robust governance structure for control of the SCR as a whole, including some kind of authoritative body to make evidence-based decisions.**
  - Any governance body should include consumer and clinician representation, have ready access to information privacy expertise and its findings and decisions should be accessible to the public wherever practicable.

- **All agencies setting up SCRs should conduct a privacy impact assessment (PIA).**
  - The Office of the Privacy Commissioner's *PIA Handbook*[3] outlines a step by step process for conducting a PIA, though following this exact process is not obligatory.
  - PIA reports should be consulted on with stakeholders (clinicians, consumers, OPC) and made public when completed.

- **SCRs need to provide for monitoring of use and auditing of key safeguards**
  - Monitoring should include both automated 'sanity checks' for outliers as well as both random and reactive checks
  - Governance bodies should approve an audit strategy and ensure they occur, as well as reporting on routine and exceptional audit activities and outcomes

[3] http://www.privacy.org.nz/assets/Uploads/Privacy-Impact-Assessment-Handbook-June2007.pdf

- **There should be a culture of privacy promoted by all participating health agencies/stakeholders which will include the positive promotion of privacy in the workplace as well as significant and consistently enforced penalties for deliberate or negligent misuse, including dismissal and complaints being laid with relevant bodies (OPC, Medical Council, Nursing Council).**
    - SCRs have a very wide potential roster of users and many potential vectors for unauthorised disclosure of health information; if consumer and clinician trust is to be maintained it is vital that misuse is absolutely forbidden and that this prohibition is stringently enforced.

SECURITY STANDARDS

- **Agencies that operate and use SCRs should comply with the Health Information Security Framework (HISF)[4]**
    - Governance bodies should take responsibility for ensuring that participating agencies are meeting their HISF obligations
    - OPC is currently assessing whether some form of independent assessment of HISF compliance would be practical and appropriate.

4 http://www.ithealthboard.health.nz/sites/all/files/10029.1%20HISF%2C%20Essentials%20and%20Recommendations%20v3.pdf

Introduction

> *Shared health care needs shared health information. But sharing needs to be justified and proportionate if it is to maintain trust – there needs to be a balance. Health information is deeply personal to all of us.*[5]

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

- *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.*[6]

A wide range of small and large scale electronic record projects are being developed to meet the National Health IT Board's 2014 deadline. Many of these projects have been reviewed on some level by the Office of the Privacy Commissioner. In general our experience has been that they demonstrate an appropriate level of concern for the privacy of health consumers, and that the agencies developing them are eager to make any necessary changes to address privacy shortfalls.

While surveys indicate that the New Zealand public has a very high level of trust in how the health sector handles its information, it might only take a few high profile data breaches for that trust to evaporate.[7] The full benefits from electronic health records can only be achieved if health consumers maintain their current high level of trust in the way their information is held, used and disclosed.

> *Nearly every interaction with an agency generates information. Mostly that information will be trivial (though even trivial data can reveal a surprising amount about the person to whom it relates). When it comes to health information, though, there is little we would consider to be trivial. Because of this, we are used to information about our health being treated in particular ways.*
>
> *We expect it to be considered as **confidential**, because in all likelihood it was collected in a situation of confidence and trust. We want it to be treated as **sensitive**, because it may include details about our body, lifestyle, emotions and behaviour. And we accept that a piece of information may have **ongoing use** if it becomes clinically relevant in the future, long after it was initially collected.*[8]

[5] Marie Shroff, address to HINZ Conference 2011
[6] National Health IT Plan, 2011. An update for 2013/14 has been released: http://www.ithealthboard.health.nz/sites/all/files/national-health-IT-plan-update-2013-14-nov13%20-%202.pdf
[7] Survey link : http://www.privacy.org.nz/assets/Files/Surveys/UMR-Omni-Results-Mar-14-Pdf-version-A349546.pdf
[8] Health Information Privacy Code 1994, page 2, 2008

These three aspects of health information – confidentiality, sensitivity and the potential for ongoing use -- are critical to assessing how SCRs accomplish the important but difficult task they set for themselves.

Another crucial issue is trust. Health care occurs in an environment that requires, and expects, a high level of trust. Patients need to be able to trust their care providers, and providers trust that other providers will properly manage the information that they hold.

Trust is created by **control** and **transparency** in the context of an ongoing relationship. It takes time to build but can be damaged in very quickly. Good management of health information also depends on **standards**, **governance** and careful attention to **security**.

Methodology

The goal of this paper is to establish what privacy lessons were learned by three SCR projects, how identified privacy risks were mitigated, and then to use that information to draw conclusions about whether EHR projects being properly assessed for privacy risks and, if not, what should change, and to provide clear recommendations for appropriate minimum standards for SCRs.

Three SCR projects were reviewed:

- Compass Health SCR ("Compass SCR")
- Canterbury DHB Electronic SCR ("eSCR")
- HealthLink Care Insight ("Care Insight")

The documentation reviewed included:

- PIAs
- Consumer privacy statements
- Framework documents
- Business cases

We also drew on discussions with project teams, practitioners and health consumers. We used this information to help assess how the projects:

- Foster and maintain transparency around collection, goals and practices
- Keep health information held by the project secure
- Institute protections against function creep
- Properly govern health information once collected

Why do we need SCRs?

Traditionally, sharing of patient information between health practitioners has occurred by referral letters, discharge summaries and verbal summaries of specific aspects of care. However these methods of shared care rely on the patient first being referred or discharged. Where an admission is 'acute', or unplanned, no information may be available apart from the bare-bones details on national registers such as the NHI and National Medical Warning System. By way of example, in 2009 around 80% of Palmerston North hospital emergency department presentations were acute.[9]

An electronic SCR allows multiple health professionals to have access to a given patient's information at the same time. It can give clinicians and patients easier access and greater control over health information which can, in turn, increase the accuracy of information held by clinicians and patients' trust in those clinicians.

Another of the drivers for developing an SCR is economic. Around the world, countries are grappling with the fact that health care is going to cost more than they can afford to pay. To manage this, health funding agencies need to do more with less. One way to accomplish this is by setting up electronic health records to reduce duplication of effort and help avoid error.

A third important reason for going electronic is that medical care, and the way it is delivered, has changed. A John Hopkins clinician determined that a hospital patient in the 1970s in the US would see, or have their information seen by, 2.5 health professionals.[10] The equivalent number today is closer to 19.[11] While traditional methods of information sharing still work in a shared care environment, they add in considerable friction to providing care; an effective SCR may be able to lessen this friction.

[9] http://www.hinz.org.nz/uploads/file/2012conference/Papers/P7_MacRae.pdf
[10] http://www.newyorker.com/online/blogs/newsdesk/2011/05/atul-gawande-harvard-medical-school-commencement-address.html
[11] http://www.prnewswire.com/news-releases/survey-patients-see-187-different-doctors-on-average-92171874.html

Confidentiality and privacy – the legal background

> ***CONFIDENTIALITY:*** *Pertains to the treatment of information that an individual has disclosed in a relationship of trust and with the expectation that it will not be divulged to others in ways that are inconsistent with the understanding of the original disclosure, without permission*
>
> ***PRIVACY:*** *Control over the extent, timing and circumstances of sharing oneself with others*[12]

Confidentiality traditionally occurs in a relationship between a patient and a clinician sitting in a room talking to each other. Shared electronic health records by contrast, are potentially available to anyone in the world with the appropriate credentials, can be downloaded almost instantly, and the information on them can be much more easily aggregated into a large dataset. This allows widespread and damaging accidental or malicious disclosures, and also increases the likelihood that secondary uses will be found, beyond the original purpose for which the information was collected – 'function creep'.

While it is much easier to record and track who has accessed an electronic record rather than a paper record, without robust governance and a well-entrenched culture of privacy this does not increase the security of the record. Unauthorised access must be noticed and reported, disciplinary processes must be followed through and the results must be publicised if they are to have any deterrent effect.

Ultimately the risk is that shared electronic records, while improving the care that can be provided to patients, can dilute the relationship of confidentiality between patient and clinician.[13]

In New Zealand law clinical confidentiality is enforced in two main ways. The first is in the consumer right to ethical treatment found in Right 4(2) of the Code for Health and Disability Service Consumers' Rights (the Health and Disability Code). The second is in rule 11 of the HIPC. Section 22F of the Health Act 1956 is also relevant, and requires any person holding health information to disclose that information, on request, to another person who is providing health care or to a patient's representative.

The HIPC rules around collection of health information are also important. Health information must be collected for a lawful purpose connected with the collecting agencies functions (rule 1), directly from the patient (rule 2) and the patient must be told the purpose for collection and who is likely to see the information (rule 3).

[12] http://www.research.uci.edu/ora/hrpp/privacyAndConfidentiality.htm
[13] http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1832055/

While the primary purpose of collection of health information in a treatment context is nearly always 'to provide care', there are often secondary purposes such as reporting provision of care to funding agencies, authorised clinical audit, planning future services and research.

Rule 3 requires the agency collecting the information to inform the individual how their information is to be used and disclosed. This agency will generally be the GP or treating clinician, rather than the 'upstream' agencies such as DHBs, PHOs or the Ministry of Health, that are using the information for the secondary purpose. Communication of purposes, for example by a privacy statement on a PHO enrolment form, is often the only avenue for ensuring that the patient is aware of how their information is to be used.

There is no legal obligation for upstream agencies to be transparent to the patient about how and why they are collecting information, but if trust between the elements of the health sector is to be maintained, purposes for collection must remain clear at all levels. Upstream agencies need to take appropriate care to ensure that the collecting agencies know where their patients' information is going, so the collecting agencies can in turn advise their patients.

Also, because a doctor who consults an SCR to obtain information about his or her patient is not collecting information directly from that patient he or she must be able to rely on one of the rule 2 exceptions. The key exceptions are where:

- The patient or their representative has consented[14]
- The patient is not able to give their consent (unconscious, incapable)[15]
- Failure to consult the record would prejudice the interests of the individual or anyone's safety[16]

[14] HIPC rule 2(2)(a) and (b) – the representative can be consulted where the patient is "unable to give their authority".
[15] HIPC rule 2(2)(d) – "compliance is not reasonably practicable in the circumstances of the particular case".
[16] HIPC rule 2(2)(c)

Elements of Trust

Health care occurs in an environment that demands a high level of trust. Patients are obliged to trust their care providers, and providers need to trust that other providers will properly manage the information that is entrusted to them.

Trust is established by **control** and **transparency** in the context of an ongoing relationship. It takes time to build but can be damaged in very quickly. Trust also requires robust **governance**, and that information is protected by appropriate **security standards.**

CONTROL

Privacy rights are intended to give people some control over their information in the face of technological developments that lessen that control. It can be useful to think of privacy in this way because it moves the focus away from the law and on to technological and social methods of increasing people's control over their own information.

The SCRs reviewed here attempt to strike a balance between creating a shared care record that is clinically useful (accurate, timely, relatively complete) and one that respects the wishes of the people whose information it contains (easy opt-off, patient audit, online access). Swinging the pendulum further towards patient control, for instance by requiring patients to opt-in to having their information placed on their shared care record, would reduce the amount of patient information held on the record very significantly and make the record much less useful to clinicians.

However decreasing patient control means that a patient may have no idea their health information is held on the record. A patient who discovers that the health information they have chosen to place in a trusted repository has been disclosed against their will is an undesirable thing. Having that information disclosed without their knowledge from somewhere it was placed *regardless of* their wishes is considerably worse.

The SCRs reviewed all recognise that all health information is sensitive, but that some health information is particularly sensitive. However, the degree of sensitivity, and therefore the harm and level of risk is subjective. While sexual health, mental health and drug addiction are areas where there is an obvious level of heightened sensitivity, the sensitivity of a piece of health information can only be determined by the individual to whom it pertains.

There are three challenges to accomplishing this:

1. Ensuring patients understand their information is held by a practice which can include information placed on their SCR by other agencies.

2. Working with the patient to ensure that the SCR is as accurate as possible

3. Understanding that patients may particularly want to control mental health and sexual health records. There is therefore a risk that the information is partially accurate, with potentially significant clinical consequences which patients need to understand. For example the interplay of some sexual health drugs can have significant effect (including life threatening) on other drugs.

Because patient and clinician trust has to be maintained in the face of a much greater scope of access to confidential information, SCRs must be able to:

- recognise health information that is of heightened sensitivity for a given patient
- effectively address the heightened sensitivity with technical or operational protections
- ensure that these protections do not present a risk to the future safety of the patient.

The SCRs all meet these requirements to some extent, but appropriate ongoing governance is required to ensure they continue to do so.

Health information in New Zealand is retained for a long time. The legal minimum is ten years from last clinical encounter.[17] Information held by a public sector organisation is subject to the Public Records Act and is under the jurisdiction of the Chief Archivist, which may mean there are specific retention requirements.

These retention requirements overrule the presumption in rule 9 of the HIPC that information will be disposed of when no longer required and, in conjunction with the ability for electronic health information to be stored very cheaply[18], mean that health information will be retained indefinitely by the SCRs reviewed.

The ongoing use of electronically held health information presents twin possibilities. On one side, electronic records are valuable for people who move between regions, reducing duplication of information and increasing accuracy. On the other side, the existence of large collections of updated, accurate and personally identifiable health information

[17] Health (Retention of Health Information) Regulations 1996
[18] Since 1980 the cost of storing a gigabyte of information has gone from $US 437,500 to $US 0.05: http://www.statisticbrain.com/average-cost-of-hard-drive-storage/

increases the temptation, and the likelihood, that additional uses will be found for that information: a phenomenon known as “function creep”.

Research and systems improvement are both publicly beneficial activities that depend on data, but these SCRs need to recognise how acting on these temptations risks damage to public trust in the record and potentially in the health sector as a whole.

While the SCRs reviewed here recognise the potential for health information having ongoing uses, they need to continue to be alert to and address the issue of function creep with regard to intended and possible future uses, for instance by requiring privacy impact assessment and/or public consultation before expanding the scope or intended uses of information held.

Shared Care Records like the ones reviewed here are not full health records. They generally exclude the most personal and detailed information held on GP records, patient notes and records of meetings. Nonetheless, the SCR takes information that was previously accessible only through the mediation of a health professional, or by making a lawful access request, and makes it accessible to anyone with the ability to access the system.

This enables convenient, effective and economical health care. However it also raises the stakes for clinicians by diluting the personal relationship that is inherent in confidentiality. A Shared Care Record must overcome this by incorporating sufficiently clear business rules to determine where disclosure is justified.

Recommendations

- **SCRs should allow patients and clinicians to easily opt out if they wish.**
  - For instance: 0800 free phone line, via GP.
  - Consequences of opting-off (e.g. that certain kinds of care may be made more difficult or that the patient may be put at increased risk) should be stated in clear but not alarmist way.

- **Secondary purposes should be minimal and tightly regulated to help maintain clinician and consumer trust.**
  - SCRs hold information on behalf of the clinicians who provided the information and the primary purpose is always to provide high quality care to patients.
  - Secondary purposes such as service improvements, teaching, research and audit must be well-publicised and use anonymised or pseudonymised data wherever possible.
  - Any new secondary purposes should only be adopted with proper consultation and with careful consideration of the potential risk to public trust in the SCR.

- **Users of the SCR should only access the record with patient permission unless a justification exists for doing so under rule 2 of the HIPC.**
  - Repeatedly obtaining permission is not necessary, nor is obtaining permission where not reasonably practicable or where it would prejudice the interests or safety of the patient.
  - A 'tick box' screen requiring users to confirm that they either have patient permission or another justification exists for accessing the SCR, and recording the result, is an appropriate protection.

- **All data access and use should be recorded and retained.**
  - Automatic recording of information about every access to an SCR ('footprinting') is an important safeguard against misuse.
  - While standards for retention of footprint information are still being developed, retention for a minimum of two years is a reasonable expectation.

TRANSPARENCY

Transparency means operating in such a way that it is easy for other to see the actions performed. There are two aspects to transparency, the first is the need to give patients access to health information about themselves, the second is taking steps to communicate intended uses of their information.[19]

Prior to the passage of the Privacy Act in 1993, as-of-right patient access to their own files was often resisted for professional cultural reasons but also for practical ones.[20] Although a paper record can be copied and disseminated, there is significant effort involved, effort which increases sharply with the size of the record.[21]

All three of the SCRs reviewed here took steps to raise public awareness of the development of the electronic SCR, and to inform the public about the ability to opt-out. The Compass SCR examined different methods of informing the public and found that there was minimal difference between a general public awareness campaign and a direct mail drop to every participant. In both cases awareness rates and opt-outs remained low. This suggests that agencies operating SCRs need to continue to make information available to consumers on how the SCR functions throughout its lifetime, for instance by use of posters in waiting rooms or making brochures available and by either notifying patients and their GPs when an external lookup has occured or making it as easy as possible to obtain that information. The Care Insight system has a natural advantage in

[19] https://www.privacyassociation.org/media/pdf/knowledge_center/EHRs_Miron-Shatz_Elwyn.pdf
[20] Baldry M, et al. Giving patients their own records in general practice: experience of patients and staff. *Br Med J (Clin Res Ed)*1986;292(6520):596-8.
[21] Rosenham, H. Patients' Rights to Access their Medical Records: An Argument for Uniform Recognition of a Right of Access in the United States and Australia, *Fdhm Intl Law Journal*, 1997, 21: 250

this respect, because its consent approach requires individuals to be informed about the system each time it is used.

Computerised SCRs, like the ones reviewed here, have potential for much increased transparency as they allow audit functionality, by way of 'footprinting' or access logging, to be exposed directly to the individual concerned. Direct patient access also allows for faster and more thorough correction of information by the individual. Patient portals are currently being implemented.

However transparency resulting from distributed access to the SCRs carries with it a significantly increased security risk, simply by virtue of the increased potential for malicious attack by having more computers with access to the information.[22]

The second aspect of transparency is ensuring that patients and clinicians are aware of the purposes for which information is being held on these SCRs. The potential scope of secondary purposes for an accurate, up-to-date and well-organised health dataset is very wide and the benefits are significant, but it is vital to the ongoing success of electronic health records in New Zealand that these secondary purposes are accurately communicated both to patients and clinicians. Trustworthy SCRs:

- take appropriate steps to ensure both clinicians and patients are aware of rules around disclosure
- have adequate governance over how these rules are enforced

All three SCRs reviewed here emphasise that the systems are only to support the delivery of care, and that the information they contain is not available for secondary purposes. While this is positive, it is not yet clear that these limitations are embedded in governance structures for the SCRs, and that they will be maintained over the longer term. Because it has adopted a distributed model, Care Insight may be less suitable for providing data for secondary purposes, as it does not provide or facilitate an aggregate view of data.

SCRs should also be transparent about the steps they have taken to protect patient privacy, in order to demonstrate that patient privacy has been carefully considered, and fostering trust as a result. Care Insight and Compass Health have both published their Privacy Impact Assessments. The Canterbury eSCR relies on a privacy framework[23].

The agencies using the SCR such as GP practices, all have a legal obligation to take reasonable steps notify their patients under rule 3 of the HIPC about the existence of the parameters around the SCR. This would include, at a minimum, ensuring that posters are prominently displayed, that brochures are available, and that over the medium term (1-2

[22] http://www.nap.edu/openbook.php?record_id=5595&page=55
[23] Available on https://healthhub.health.nz/escrv/healthcareproviders.html for clinicians and https://healthhub.health.nz/escrv/publicandpatients.html for public

years) most or all of their patient base has been directly notified. For instance, an electronic mailout to all patients with email addresses on file could be followed up by inserting brochures into mailed out bills.

Recommendation

- **Agencies operating the SCR must provide resources that make it as easy as possible for participating agencies (e.g. GPs, hospitals, testing laboratories) to publicise the existence of the SCR and the parameters around its use.**
  - At a minimum this would include brochures and posters in GP waiting rooms and readily accessible websites with clear Plain English explanations of the SCR.
  - Training for staff is also vital, in conjunction with an overall culture of privacy, to ensure that patient questions can be answered and concerns addressed
- **Primary health care providers such as GPs that are using SCRs should take reasonable steps to notify their patients about the existence of the SCR and the parameters around its use**
  - For instance keeping stocks of brochures updated, posters prominently displayed, and conducting low-cost population notification by email or adding an explanatory brochure when sending mail to patients.
- **Agencies operating the SCR should publish their privacy analysis underpinning the privacy safeguards of the SCR.**

GOVERNANCE

Governance of health information is also vital to ensuring the trust of those to whom the information relates. In practice this entails having a structure for control of these SCRs as a whole, including some kind of authoritative body that has responsibility for making decisions about the system, and to ensure that norms developed for the SCR during the development stage are consistently enforced. Failure to do this can see privacy safeguards eroded by subsequent development of the system.

Both the Compass Health and Canterbury eSCR have dedicated structures that govern the SCR's operation.

A Privacy Impact Assessment (PIA) is an important tool for setting up the structures that will govern the flow of information once a system is implemented. A PIA should identify key risks to privacy and identify appropriate mitigations. In its final form, it should provide an ongoing catalogue of privacy safeguards and the reasoning behind them. This in turn provides a useful guide for measuring, reporting and ensuring that these safeguards are not eroded by the future development of the system.[24]

[24] The Independent Review of ACC's Privacy and Security of Information provides an excellent overview of what a high quality security and privacy culture would look like: http://privacy.org.nz/assets/Files/Media-Releases/22-August-2012-ACC-Independent-Review-FINAL-REPORT.pdf

Effective auditing of, and reporting on, controls established to secure privacy is also a critical part of the governance toolkit. The value of controls is undermined if there are no checks to ensure they are complied with.

Agencies operating SCRs also need to provide effective penalties for misuse of SCRs. Each of the SCRs reviewed here operates within a wider disciplinary framework that falls outside the scope of this review. Nevertheless, it is important to stress that there need to be effective sanctions for misuse, in conjunction with a robust culture of privacy supported by appropriate policies, procedures and training.

- **There must be a robust governance structure for control of the SCR as a whole, including some kind of authoritative body to make evidence-based decisions.**
  - Any governance body should include consumer and clinician representation and its ongoing reporting of activities, findings and decisions should be accessible to the public.

- **All agencies setting up SCRs should conduct a privacy impact assessment (PIA).**
  - The Office of the Privacy Commissioner's *PIA Handbook*[25] outlines a step by step process for conducting a PIA, though following this exact process is not obligatory.
  - PIA reports should be consulted on with stakeholders (clinicians, consumers, OPC) and made public when completed.

- **SCRs need to provide for monitoring of use and auditing of key safeguards**
  - Monitoring should include both automated 'sanity checks' for outliers as well as both random and reactive checks
  - Governance bodies should approve an audit strategy and ensure they occur, as well as reporting on routine and exceptional audit activities and outcomes

- **There should be a culture of privacy promoted by all participating health agencies/stakeholders which will include the positive promotion of privacy in the workplace as well as significant and consistently enforced penalties for deliberate or negligent misuse, including dismissal and complaints being laid with relevant bodies (OPC, Medical Council, Nursing Council).**
  - These SCRs have a very wide potential roster of users and many potential vectors for unauthorised disclosure of health information; if consumer and clinician trust is to be maintained it is vital that misuse is absolutely forbidden and that this prohibition is stringently enforced.

[25] http://www.privacy.org.nz/assets/Uploads/Privacy-Impact-Assessment-Handbook-June2007.pdf

SECURITY STANDARDS

A standard is a set of guidelines that applies across a sector or field of activity. In the health sector, the Heath Information Standards Organisation (HISO) has issued 15 approved standards, and has endorsed a further 9. The standards are generally technical and allow different organisations to share and use the same information.

The Health Information Security Framework (HISF) was issued by HISO in 2009, along with the related document *Guidelines for Small Organisations.* [26]

Key elements of security covered off in the methodology include:

- *An information security policy document*
- *Allocation of responsibilities for information security*
- *Awareness, training and education*
- *Appropriate management of technical environment*
- *Business continuity management*
- *Recording incidents and implementing improvements*

The standard sets out a reasonable baseline for small to medium size organisations to securely manage the health information they hold. Rule 5 of the HIPC requires agencies holding health information to take reasonable security safeguards against unauthorised access, loss, use, modification and disclosure; expectations for reasonable security safeguards, and therefore compliance with Rule 5 of the HIPC, should start with HISF compliance as a minimum.

Compass Health specifies application of the HISF for the storage and transmission of information. Care Insight and Canterbury eSCR do not mandate the use of the HISF, but rather set out high-level expectations of users that are intended to accomplish the same goal. We consider that all three SCRs should be more demanding. Any system that connects to the shared care record can be the source of an attack or loss, and therefore any connecting system should be compliant with the relevant standard.

We have identified that there is a gap in identifying overall levels of compliance with the HISF in the health sector and this presents some concerns. But it is not the role of SCRs to remedy this gap, and we are considering how else it might be filled.

[26] http://www.ithealthboard.health.nz/hisf

- **Agencies that operate and use SCRs should comply with the Health Information Security Framework (HISF)[27]**
  - Governance bodies should take responsibility for ensuring that participating agencies are meeting their HISF obligations
  - OPC is currently assessing whether some form of independent assessment of HISF compliance would be practical and appropriate.

Is our trust in the standard of 'acceptable privacy protections' in regional SCRs justified?

As discussed in the appendices, these SCRs share the following qualities:

- Online summary care record based on GPs' computerised Practice Management System (PMS)
- Public notification of existence of system by way of posters and pamphlets in GPs offices
- Easy access to opt-out facility for patients
- Summary of health data online via secure network, with potential for addition of more sensitive information at a later date
- Accessible by authorised health professionals via password/login with permission or as needed to provide care where permission is not available
- No intentional provision for secondary purposes beyond health care
- Eventual provision for patient access to their own information via password/login
- Footprinting of all data access and alteration
- Manual and automated scrutiny of data access
- Consequences for misuse of information, extending beyond being removed from the system

Compromises between patient control and convenience for clinicians are inevitable, but the nature of the compromise needs to be carefully scrutinised. Taken as a whole, this could be seen as a reasonable set of compromises. However if any of these protections and positions are weakened, then the whole structure can lose its integrity.

A compromise that is reasonable can easily become an intrusion if opting out of any of these SCRs becomes harder, for instance, or if full information is placed online. Similarly, a compromise can be jeopardised by secondary uses of the data, or if footprint data showing malfeasance is not reviewed and acted on promptly,

A more fault tolerant system that engineers privacy more tightly into the system's design could have merits.

[27] http://www.ithealthboard.health.nz/sites/all/files/10029.1%20HISF%2C%20Essentials%20and%20Recommendations%20v3.pdf

For instance, the Care Insight SCR explicitly does *not* create a central database of health information, avoiding several of the potential problems (function creep, large-scale data breach) to which a centrally located database is potentially subject. This is a 'privacy by design' approach in the sense that it removes the temptation for local, regional or central government health authorities to utilise collected patient information in new and unexpected ways.

This compromise is not without a price, of course: access via Care Insight to a GP's system requires that the GP's system be functioning and accessible. While a centrally located, professionally maintained data storage centre might also be knocked out this would likely require a large earthquake or other major natural disaster.

Are the SCRs being properly assessed for privacy risks?

Based on the assessments set out in the appendices, and without prejudicing any views the Privacy Commissioner may choose to form in the future, the three SCRs appear to be well-managed projects that have accomplished their clinical goals while complying with their obligations under the HIPC. The PIA reports they have produced do an acceptable job of outlining the potential privacy risks and proposing mitigation strategies.

While there are reasonable questions that might be asked around ongoing governance, most of these will only become pertinent as SCRs become a commonplace part of the health landscape. Currently, that landscape is one in which health consumers have a very high level of trust in their health providers. Decisions made by Compass SCR and Canterbury eSCR (e.g., the decision to populate their database without seeking specific patient permission) reflect that sympathetic environment.. Care Insight's method, of avoiding a central database and accessing information as needed for each enquiry, will possibly prove more robust in the event that public trust in the health sector wanes, though may represent a higher level of risk to ready access to information in the event of another major catastrophe such as the Christchurch earthquakes.

For the time being, and with the context of national governance principles being developed by bodies like the Health Information Governance Expert Advisory Group, this question can be answered with a guarded 'yes'.

Appendix 1: Compass SCR

> *The "Better, Sooner and More Convenient" (BSMC) initiatives are primary care led initiatives that are intended to create transformational change in the health sector to improve the health of patients. These initiatives were begun in the various health districts around the country at the beginning of 2010, including in the Wairarapa and MidCentral DHBs.*

The Compass SCR is an electronic summary SCR, based on the MedTech ManageMyHealth platform and operating throughout the Central region of New Zealand. The project covers around 10% of New Zealand's population.

The Compass SCR takes a specified set of summary information uploaded by GPs from their Practice Management System (PMS), stores it in a local cloud facility operated by MedTech, then makes that information accessible to authorised local care providers and to the patient in a read-only format.

Currently there are 45 practices supplying information to the Compass SCR in the Wararapaand Capital and Coast DHB areas; around 80% of patients in those regions have a record in the Compass SCR. The data supplied to the online record is:

- Prescribed Medicines
- Problem List (Diagnoses, Conditions)
- Allergies
- Immunisations
- Recalls
- Laboratory Results[28]

While there are no specific plans to expand this list to include, say, patient notes, the technical potential for expansion does exist in the ManageMyHealth software package.

How is Compass SCR populated?

In order for an SCR to be usable, it needs to contain information for a large proportion of the relevant population. If this is not the case, busy professionals will be less likely to use the record.[29] A challenge that is common to all SCRs is getting the necessary information onto the record, 'populating' the database.

[28] This can include various forms of electronic health information; e.g. radiology results, specialist letters and notes from District Health Boards

[29] One of the reasons identified for the failure of the UK NHS Summary Care Record is that clinicians regularly did not find the information they were seeking, and so were unwilling to use the record:

The Compass SCR was populated on the basis that all patients on the PHO's population register would have their information transferred unless they opted out or their GP opted out for them. However once the initial transfer had taken place, further transfers would be on an 'opt-in' basis. A number of safeguards were used to mitigate the risks associated with wholesale transfer of information.

1. Each participating GP was provided with a query tool that helped to highlight patients with particularly sensitive data. This was run by each GP on the data in their own PMS, and highlighted sexual and mental health issues that might need to be held back from the record.

   Comments

   - This approach gave considerable autonomy to the health practitioner with the most direct clinical relationship with the patient, the patient's GP.
   - However there is no guarantee that any given GP would have done a searching audit of their patients' data to assess confidentiality issues.
   - Providing a query tool is a useful tactic for creating greater certainty than an ad hoc survey by the GP of their own records, while still leaving the decision about the scope of the review in the GP's hands.

2. A communication plan that informed health professionals and patients about the intended transfer was prepared.

   Comments

   - Communicating the substance of any project that significantly affects a target population should be considered a minimum standard.
   - This is of particular importance when, as is the case with the Compass SCR, an opt-off approach is being used.
   - Compass took additional steps to assess the effectiveness of different modes of notification by comparing them with numbers of patients opting out.[30]
   - Its findings indicated that there was a 'shelving effect' where additional resources put into notification did not significantly improve overall awareness.

3. Patients were placed on the Compass SCR without obtaining their consent, except from the generic consent on their PHO enrolment form. They were given the opportunity to opt-off (and advised they could opt off, and back on, at any time in the future)

[30] reference to compass research

Comments

- The ability to opt on/off is popularly considered a right with information systems, but is not *explicitly* required in law, as there is a wide range of possible ways that health information may be legitimately disclosed without the permission of the individual.
- Rights of access and correction under the HIPC give people additional control over their information, but not to the point of conferring the right to opt off an electronic system that holds health information.
- That said, rule 2 of the HIPC requires health agencies collecting information from a source other than the patient to obtain the patient's permission unless there is another permissible ground for the collection.[31]
- It is important both for reasons of increased patient autonomy and patient trust that there is a robust ability to opt out of participation.
- This is complicated, however, by the clinical factor. Although clinicians are trained not to treat any record as necessarily complete and accurate without independent confirmation, if a patient has completely opted out of having their health information displayed there is a chance that the clinician may miss vital information. There is a balance to strike between patient autonomy and clinical efficiency.

4. Patients and GPs were given the opportunity to designate any aspect of the information held on the PMS as 'confidential', preventing it from being uploaded to the Compass SCR.[32]

Comments

- In privacy law, there is little distinction between sensitive and non-sensitive health information.[33]
- This lack of distinction does not necessarily reflect the way people actually view their own health information.
- One of the key advantages of electronic records is the ability to filter and segregate records with certain characteristics. This is of particular importance

[31] Rule 2, HIPC. Permissible grounds include that the purpose of collection would otherwise be prejudiced, that direct collection is impracticable in the circumstances of the particular case, or that direct collection would jeopardise someone's safety

[32] Compass Health commented: ""Confidential" has a specific function in MedTech and is often criticised as a term because all clinical health information is 'confidential'. MedTech have added the concept of 'exclude from MMH' to differentiate 'confidential' information from that which patients do not wish to have included as part of their SCR. The 'confidential' flag is used within a practice to make certain pieces of clinical information not available to all clinical staff. This is practically used for the highest and most sensitive data."

[33] The HIPC applies to any health information about an identifiable individual; the exceptions to the HIPC rules provide a structured method for determining whether or not information can be legitimately disclosed. Sensitivity of the information can have a bearing on the nature and extent of any harm resulting from a privacy breach, however.

when it comes to confidential records, as it allows information with particular sensitivity, such as sexual and mental health records, to be designated as such.

5. A privacy impact assessment was conducted and a peer-reviewed report issued.

Comments

- A privacy impact assessment is a structured process for moving through the potential privacy risks and suggesting (or ruling out) appropriate mitigations and privacy enhancing responses.
- The Compass SCR PIA report states its goals as being to:
  - *identify the potential effects an electronic summary SCR may have upon individual privacy;*
  - *identify the potential effects using ManageMyHealth to provide access to a summary SCR 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.*[34]
- The Compass SCR PIA report is described in more detail below.

How does Compass SCR demonstrate transparency?

The Compass SCR framework for releasing the SCR was:[35]

- *Primary Socialisation – introduce the idea*
- *Hospital Agreement – ensure they'll use it*
- *Secondary Socialisation – introduce the idea*
- *Primary Sign-Off – recruit practices*
- *Public Awareness – information sharing*
- *Sensitive Code Review – selectively review data*
- *Data Upload – push data into the cloud*
- *GP Only Access – let GPs review what's there*
- *User Acceptance Testing – check what's there is correct*
- *Provider Training – show everyone how to use it*
- *Go Live*

[34] Compass SCR PIA, p2
[35] http://gpnz.org.nz/wp-content/uploads/Compass_Learning-from-Shared-Care-Record-Implementations-and-Chronic-Care-Procurement.pdf

Consumer awareness was handled, variously, by mail outs and brochures/pamphlets in the participating GP practices. In the Wairarapa district, a public awareness campaign was undertaken, which included media releases, direct information to all general practices, and letters to community groups. To establish which method was preferable, the Compass SCR team analysed the data around opt-outs from the system, both in areas that received a mail out and areas that did not:[36]

The analysis concluded that the overall opt-out rate was very low (on the order of 20-40 per 100,000 population), that notification was most effective within 8 weeks then trailed off sharply, and that there was minimal difference between a general public awareness campaign and a direct mail drop to every participant.

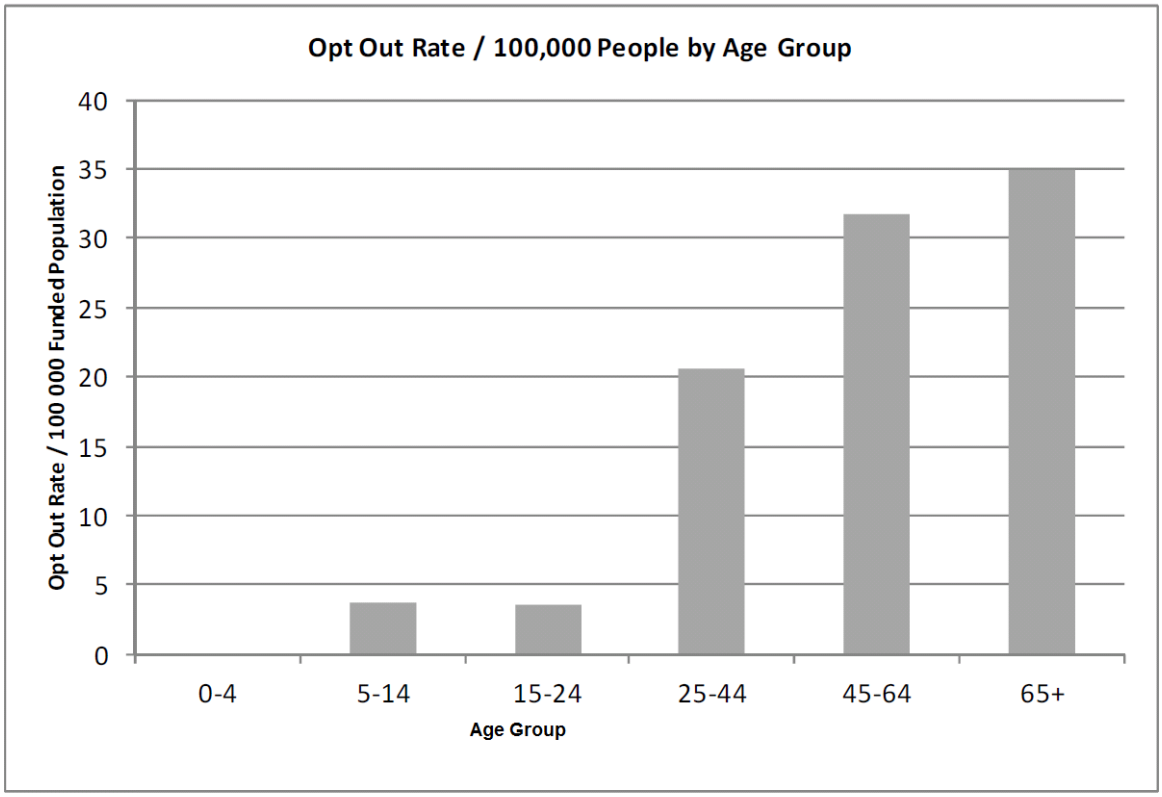


Figure 3 - Opt Out Rate / 100 000 People by Age Group

The pamphlet notifying people about the possible use of their health information set out the intended use for the information as being "to help health professionals involved in your care access pertinent information from your general practice health record. Doing this may mean that those involved in your care can make decisions with more information, which can make those decisions safer and of a higher quality than they may otherwise be."

[36] http://www.hinz.org.nz/uploads/file/2012conference/Papers/P7_MacRae.pdf

How does Compass SCR help consumers to maintain control over their own information?

Compass Health staff visited each practice that was participating in the Compass SCR to discuss the record and provided leaflets and posters setting out the anticipated creation of the SCR as well as the ability of any health consumer with concerns about the new system to have their information removed from it. They also conducted an independent research project as the system went live to assign concrete numbers around health consumers' decisions to opt-off the system, as noted above.[37]

Opt-off is by calling a free-phone number, and is 'all or nothing' – a patient is either on the record or they are not.

How does Compass SCR adhere to standards?

Use of the HISF is mandated for agencies participating in the Compass SCR by the Project Governance Group. However, in the absence of formal audit requirements and sector-wide oversight, it is open to question what proportion of agencies with access to the Compass SCR will be complying with the HISF. This is an issue that may be best addressed by reference to GP organisations such as the Royal NZ College of General Practitioners and Patients First (formerly GPNZ).

How does Compass SCR protect against function creep?

The Compass SCR approaches this problem by explicitly ruling out the subsequent and secondary use of information held on the record. Technically this will not impede any of the new purposes which might be found for the information, as the SCR is only a reflection of data held on other health systems. However the SCR presents a way to bypass the other gatekeepers of the information, and to obtain it in a much more useful form, on a region-wide basis. It also gains its value from patients in the region choosing not to opt-out from its coverage and therefore has a strong interest in maintaining their trust in how their information is being handled.

The Compass SCR also has the potential for function creep through the extension of the record into more detailed and potentially more intrusive areas. As set out above, the online record currently only holds summary information. However the ManageMyHealth product, on which the Compass SCR is based, has the capability to share any aspect of a GP's PMS. The Compass SCR online FAQ states (emphasis added):[38]

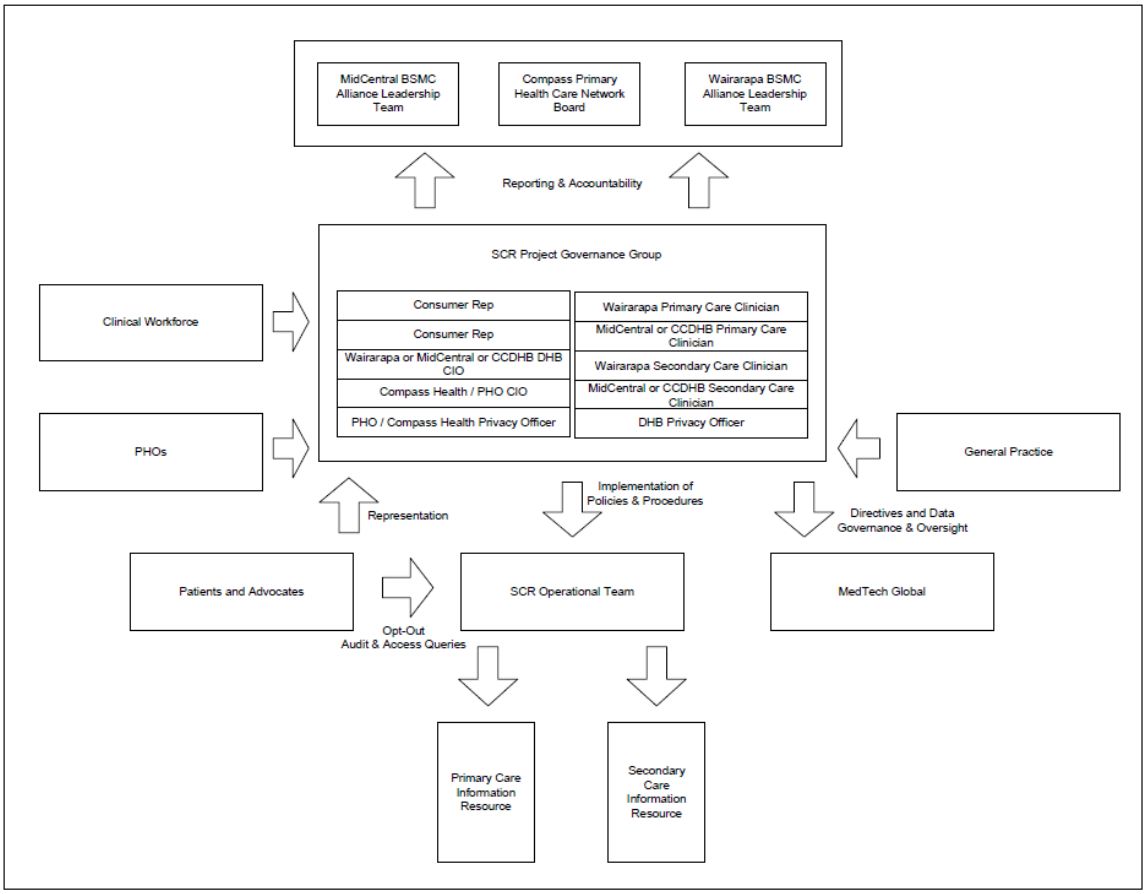
[37] http://blog.healthlink.net/wp-content/uploads/2012/09/Care-Insight-Privacy-Impact-Assessment-v0_7.pdf
[38] http://www.compasshealth.org.nz/HealthServices/SharedCareRecord.aspx

> *The consultation notes that your doctor records as part of your visit are not **currently** shared as part of this record.*
> *…*
> *ManageMyHealth is able to do more than the basic functionality we are using it for. At a later date, your general practice **may choose to use some of the other functions of ManageMyHealth**. If this happens, more information will be available to you at the time of the change.*

Much of the balance between clinical effectiveness and personal privacy is predicated on the summary information held on the record being confidential and sensitive, but not as confidential and sensitive as the detailed notes and records of interviews held by the GP. Given that it is technically possible for the latter information to be held and accessed on the Compass SCR, management of internal and external pressure to access this information is a key issue for governance into the future.

How does Compass SCR govern health information once collected?

Compass SCR governance structure during development of the system was as outlined in this diagram:



Following implementation, governance was divided up on a regional basis, with governance in the Wairarapa, Wellington and Central regions being handled by clinical sub-groups of the relevant PHOs.

There is a hidden weak point in the extensive reliance on audit of footprint data around potentially improper access to patient records. If footprints and audit are to be reliable safeguards, they must be reliably policed, which may take a significant commitment of resources. Compass SCR has indicated it is willing to do this, but as patient access becomes more widespread this is an easy commitment to let slip.

Does Compass SCR incorporate sufficiently clear business rules to determine where a justification for disclosure exists?

The Compass SCR is a tool intended to act as an adjunct to information a clinician may otherwise collect.

In some circumstances, this additional information may negate the need to discuss with a GP; in other situations it may stimulate the need for a discussion with a patient's GP:

> *This project means only to change the mechanism by which the information is shared, not whether it is shared or not. ... Treating health professionals will have the ability to view all information contained within the patient's SCR whether it is pertinent to the referral or not.*
>
> *All health professionals that are given access to this record … are required to be registered with a professional body. As such they are obliged to maintain moral, ethical and professional standards at all times. … If a patient consents to treatment within a health care facility, they are, in effect, consenting to disclosure of their SCR to health professionals treating them within that facility.*[39]

The explicit and implicit business rules around use and disclosure of information obtained from the Compass SCR are effectively identical to those around use and disclosure of information obtained from a referring doctor.

While this is a *practical* solution, in that it allows information to be used for care without additional communication or red tape, it does not necessarily provide the additional protections that individuals whose information is stored on the Compass SCR may feel they need. The promulgation of patient access to their own SCRs (and related audit logs) may help determine what, if any, additional protections are needed.

[39] Compass SCR PIA p27

Does Compass SCR take appropriate steps to ensure both clinicians and patients are aware of these rules?

Materials provided to participating GPs and to patients set out the goals of the Compass SCR and likely uses for the information in appropriate detail.

Clinicians are required to routinely seek consent for accessing the Compass SCR except where the patient is unconscious or otherwise unable to give consent[40] or where seeking consent would compromise care.

Education and awareness can be tricky things to measure accurately, and the research done by Compass SCR suggests that the benefit from additional efforts in this area can shelve off steeply.

Does Compass SCR have appropriate security around the information it holds?

Health information stored on the Compass SCR is securely stored by MedTech, under conditions that reflect the Health Information Security Framework (256 bit encryption in the database, 128/256 bit encryption on transmission via SSL).

Access to the information via the Compass SCR is not restricted apart from by the requirement that users be health professionals with an approved login.

All information access is tracked and logged, but the extent to which this will be a deterrent for misuse is dependent on how vigorously improper access is identified and pursued.

Ultimately, however, information must be accessible if it is to be used. The security of any health information is in the hands of the health professionals who are tasked with using it.

Does Compass SCR recognise health information that is of heightened sensitivity for a given patient?

The 'confidential' status flag recognises the existence of medical information on participating GPs' computer systems, as does the ability to opt off the system. There is also an option to mark certain kinds of sensitive information (prescriptions, consultation notes, alerts, results and diagnoses) as 'not to be uploaded to SCR'. This allows patients:

- to opt-out of the system entirely e.g. not have a record available at all
- to decide which items of information they wish to exclude by marking as 'exclude from MMH'.
- to have currently 'confidential' flagged information excluded from their SCR

[40] Compass SCR PIA p42

This level of control extends down to individual medicines, classifications and lab results. That said, the decision not to have an opt-on structure risks accidental unwanted disclosure of sensitive information, however mitigated this may have been by these controls and by giving GPs the option to screen their patients' data before populating the Compass SCR database.

Does Compass SCR effectively address the heightened sensitivity with technical or operational protections?

As described above, the confidentiality flag provides a way of designating health information that is recorded on a 'need-to-know' basis.

Ensuring that the confidentiality flag is applied consistently by GPs, and that the existence of the flag, and the guidelines around its use are widely promulgated and well-understood is a significant issue for the Compass SCR Governance Group.

Does Compass SCR ensure that these protections do not present a risk to the future safety of the patient?

Patients wishing to opt out of the Compass SCR are able to do so by mailed-in form, freephone or by discussing the matter with their GP

Opting out is identified as possibly meaning that clinicians will not have all the necessary information

The fact that a patient has opted out may not be visible to clinical users of the system, which may present clinical risks to the individual opting out, and these should be explained at the time that the decision to opt out of the display of some or all of the patient's clinical record is taken.

Does Compass SCR address the issue of function creep with regard to intended and possible future uses?

The Compass SCR holds a subset of the health information stored on participating GPs' PMS. To achieve the clinical benefits of participation in the Compass SCR, maintaining GP trust is critical.

Accordingly secondary use of data held on the Compass SCR for purposes other than care is explicitly ruled out.

What privacy lessons were learned by the projects – how were privacy risks identified and mitigated?

The Compass SCR was preceded by extensive consultation and a very thorough privacy impact assessment, which is publicly available.[41] In summary, it defines its terms, sets out an overview of the project, describes the information flows, addresses how each of the 12 health information privacy rules applies, and makes a set of recommendations for future action.

In addition to these aspects it also lists 14 'specific considerations' many of which are broadly applicable to projects of this type. For instance:

- Opt off mechanisms
  - Patient records are uploaded to the Compass SCR if they are enrolled in a paticipating PHO and have not opted out. This was intended to ensure maximum coverage and recognised the generally very low level of opting out (in a similar project in Scotland, with 5.4 million participants, 1,600 patients opted out). However this approach both relies on a high level of public trust in the health sector as a whole and the project specifically, and requires that appropriate efforts be made to ensure participants are aware of the project and easily able to remove themselves from it if they do not want to take part.
- Specialist and sensitive services
  - Services that deal with particularly sensitive issues should be automatically excluded from providing information to the SCR as a matter of course. This includes the sexual health services, school clinics and sexual abuse assessment and treatment services. However, information stating that information is not uploaded to Compass SCR should be made available at these locations, both to improve awareness of the SCR and to allow patients to mitigate any risks that might arise from clinicians being unaware of information held by the specialist service.
- Data quality for opted out information
  - If a patient opts out of the SCR entirely, their record will not show up at all, which will be apparent to treating clinicians, and will enable them to complete a medical history in consultation with the patient or their GP. However when a particular piece of information has been designated confidential by the patient, there will be no sign that information is missing. This can be addressed by recognising that the record is summary by nature and therefore potentially incomplete, and by educating health professionals to act accordingly. International experience suggests the risk from incomplete SCRs is low.[42]

[41] PIA link, compass website
[42] http://www.bmj.com/content/340/bmj.c3111

- Access by people of patient's choosing
  - The patient portal allows patients to show their own view of the Compass SCR to anyone they choose, allowing self-management and determination, as well as facilitating initiatives like Whanau Ora.

- Ensuring authorised access
  - Access to a patient's file, based on their NHI number, is restricted to registered health professionals operating within an approved setting. Policing of this is a matter for the Project Operational Team.

- Community Pharmacists Use of SCR
  - Community pharmacists score relatively poorly when it comes to health consumer trust. It is been suggested that this may be because non-medical people do not draw a distinction between the retail aspect of pharmacies and the reality of pharmacists as medical professionals.[43] Access to the Compass SCR may be given to community pharmacists when dispensing scripts or pharmaceutical advice. This is a potentially risky area that needs careful consideration.

- Project Scope Change
  - Project scope changes, and the task of communicating those changes to users, clinicians and the wider public are the responsibility of the Project Governance Group. This is also a significant risk area when it comes to patient trust in the integrity of information held by the Compass SCR.

- General Practice Opt-in
  - GPs must opt-in to their participation in the Compass SCR and may withdraw their patients, in whole or in part.

[43] http://privacy.org.nz/assets/Files/6257966.pdf

Appendix 2: Care Insight SCR

> *It is extremely important that there is a high level of trust among the providers in the region. Unless general practices and pharmacies agree to provide information to Care Insight, the system will not provide an adequate level of information to be of use. It is very important that the whole health care provider community is prepared to work together.*[44]

The Care Insight SCR (Care Insight SCR) is provided by HealthLink in conjunction with technology provider DrInfo. The service is delivered over the New Zealand Health Network, which is also operated by HealthLink. It is not accessible via the public internet.

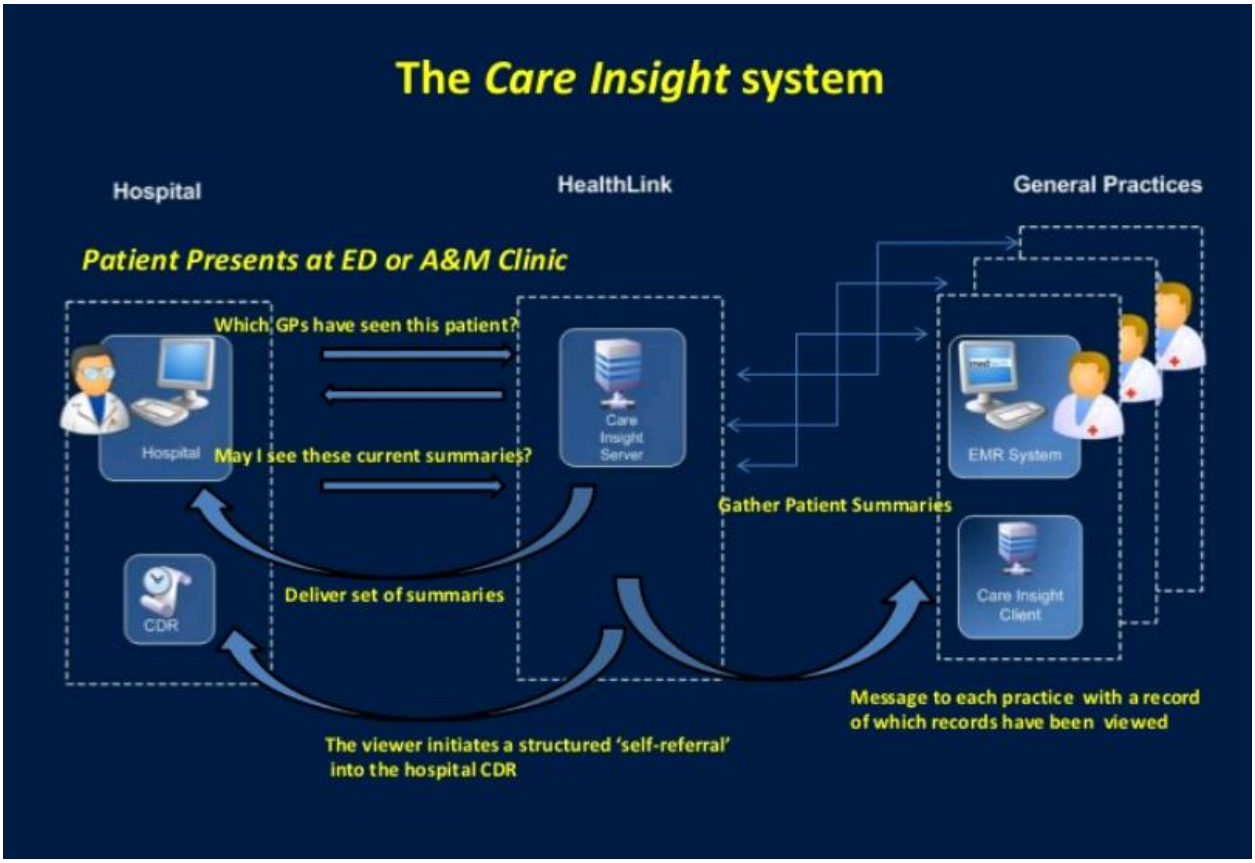
> *The Care Insight service has been designed to enable a care provider from a hospital or after-hours clinic to send an electronic request to a patient's general practice or pharmacy and receive an instantaneous summary of that patient's recent history, known medical conditions, allergies, medications and other information that may be helpful in providing them with emergency care.*

The Care Insight SCR, which has been in use in the Hawkes Bay DHB since 2011, is intended to provide a window on key data held by GPs and pharmacies without needing to extract and store that information except where necessary. The data viewed typically includes medical history, allergies, current medication and prescriptions as well as radiology and pathology reports.

> *When a patient arrives at an emergency clinic he or she is asked for approval to request information from a general practice or pharmacy. Care Insight is then opened up from within the emergency department's clinical workstation and the patient's NHI number entered. Care Insight then performs a sweep of general practices and pharmacies within the region and returns a list of pharmacies and general practices that the patient has attended within the past 12 months. At that point the patient may ask that information from some of the pharmacies and general practices not be accessed. A record summary is then requested from each of the remaining general practices and pharmacies.*

The information is presented within the web-browser of the clinical workstation as a series of reports; the information from different sources is not merged. The information may be printed. It cannot as yet be imported into the hospital's patient management system.

[44] http://blog.healthlink.net/wp-content/uploads/2012/09/Care-Insight-Privacy-Impact-Assessment-v0_7.pdf



Each practice or pharmacy that has sent patient information is automatically sent an electronic message to alert them to the fact that this information has been viewed from within their system.

Care Insight operates within the New Zealand Health Network, and can only be accessed by appropriately authorised users. Patient consent is sought immediately prior to any request for information, and a message confirming that patient record access has taken place is automatically sent to any practice that provides information.

Care Insight has been in use in the Hawkes Bay District Health Board region since December 2011.

How is Care Insight SCR populated?

The Care Insight SCR does not rely on a centralised repository of health information and therefore does not need to be populated. In one sense this is a strength as it minimises the number of large scale data transactions required to produce a functioning SCR and it reduces the likelihood of a health consumer being unhappy that their health information has been transferred without their knowledge or consent. However it does rely on multiple systems being functional and available at all relevant times, as well as providing a somewhat larger potential array of security weaknesses by entailing many more small

information transactions between GPs' computer systems, each of which represents a vulnerability; not all GPs are also skilled in information security.

How does Care Insight SCR demonstrate transparency?

This SCR is currently smaller in scope than the other two, but has also taken pains to publicise its existence, as well as the actual and potential benefits of its use.

> *The Northland PHOs IT Manager sent the initial communication from the PHO to General Practices and asked for consent forms for participation to be sent back. This was a good initiative (rather than having HealthLink send out the communications) as it was seen to be more personal coming from the PHOs which already have the trust relationship with each practice so was easily contactable for any queries, etc. As the consents came through these were emailed to the HealthLink project team who in turn contacted the practice to arrange a suitable time for installation.*[45]

Theoretically the requirement to obtain patient consent before each access request to the system would address the need for transparency around the system. In practice the Care Insight privacy impact assessment suggests supplementing this:

> *The exact usage of Care Insight will be subject to the policy of the sponsoring DHB, and the following measures are recommended:*
>
> - *Use of posters on emergency department waiting room explaining Care Insight.*
> - *Information about Care Insight use to be added to any forms given to patients upon admission.*
> - *Use of the service to be publicised in local media.*
> - *If patients do decline to have their information retrieved from GP or pharmacy systems they need to be made aware of the consequences of withholding it.*
> - *Patients can be given the option to have information retrieved from some sources but not others. Care Insight provides a list of information sources and, at the option of the patient, certain sources may be excluded from the retrieval process.*[46]

[45] http://www.pharmacytoday.co.nz/media-releases/2013/april-2013/10/healthlink%E2%80%98s-care insight-service-now-rolled-out-across-northland.aspx
[46] http://blog.healthlink.net/wp-content/uploads/2012/09/Care-Insight-Privacy-Impact-Assessment-v0_7.pdf

How does Care Insight SCR help consumers to maintain control over their own information?

While Care Insight SCR does not give consumers the ability to opt-off the system, this does has less affect on their control over their health information. Since each access is with the explicit permission of the individual, control is able to be exercised in a more granular manner, though this is dependent on the integrity of the health professionals accessing the system. Consent is tracked by the system and improper access is audited.

How does Care Insight SCR adhere to standards?

The Care Insight SCR does not explicitly mandate the use of any formal standard. Instead it provides:

> *The security of the data obtained using Care Insight is of paramount concern, and is enabled by 4 key aspects of the Care Insight service design:*
>
> 1. *Only authorised users may access Care Insight, and the system logs user access and activity.*
> 2. *All transmission of data takes place within the secure Health Network.*
> 3. *Patient consent is explicitly confirmed at point of information request.*
> 4. *An advice is sent automatically to any practice or pharmacy from which data is obtained.*[47]

How does Care Insight SCR protect against function creep?

The key protection against function creep is that a central repository of health information is not developed and retained. The Care Insight SCR acts as a conduit that accomplishes the goal of providing treating clinicians with non-geographically-constrained access to accurate patient information.

How does Care Insight SCR govern health information once collected?

The issues around governance of health information are largely avoided by ensuring that no health information is retained by the system, though HealthLink does retain records of accesses by treating clinicians.

To an extent the monitoring and enforcement of inappropriate access is 'farmed out' to the GPs involved, by way of HealthLink messages that are sent to those GPs when an access is made via the Care Insight SCR. While this has some merits in that it does not create a 'choke point' that has to review and assess all accesses, there is a risk that that

[47] http://blog.healthlink.net/wp-content/uploads/2012/09/Care-Insight-Privacy-Impact-Assessment-v0_7.pdf

GPs will not routinely review Care Insight SCR access events, particularly as use of the system becomes normalised.[48] Should this be the case, the HealthLink messages will become a useful record of access for subsequent audit, but will not significantly improve governance of the system.

The ultimate issue with a heavily consent based system is how to determine whether consent is being properly obtained each time. While a 'checkbox' approach has the merit of being simple and quick, there is a risk that it will become an automatic action associated with each use of the system. On the other hand, the number of individuals who are likely to have issues with access to GP-held summary care information is generally small and will be well aware of the importance of exercising their autonomy around access.

Does Care Insight SCR incorporate sufficiently clear business rules to determine where a justification for disclosure exists?

The Care Insight SCR requires consent from the patient be obtained and recorded before providing access to their health information.

Does Care Insight SCR take appropriate steps to ensure both clinicians and patients are aware of these rules?

Consent is a well-understood concept in the clinical world. The use of consent as the core protection should mean that clinicians will be aware of the need to obtain the patient's informed consent to access their information via Care Insight SCR, and this is supported by an obligatory 'click-through' that clinicians need to enter, stating that they have either obtained consent or consent was not able to be obtained in the circumstances.

In each case where consent is not obtained, access will be allowed but the clinician will be contacted by Care Insight and asked to provide an explanation.

Does Care Insight SCR have adequate governance over how these rules are enforced?

Consent must be recorded and the reason for any access outside the scope of consent recorded. In the event of the latter, a physical letter is sent to the accessing GP.

Healthlink emphasises that maintaining the integrity of the rules around use of health is paramount, and that it will take misuse of the system very seriously.

[48] In a response to a draft version of this report, Healthlink advised that it was actively managing this risk by working to improve the ease of use of the Care Insight inbox

Does Care Insight SCR have appropriate security around the information it holds?

Care Insight SCR provides security around the channel of transmission and a functional minimum of security (authenticated login/password) around access to one end. By notifying the GP whose system is accessed there is also a degree of 'after the fact' security.

Does Care Insight SCR recognise health information that is of heightened sensitivity for a given patient?

Where the GP has been asked, or decided, to keep certain information confidential it will not be visible to other users of the Care Insight SCR.

Where the GP has been asked to keep certain information confidential it will not be visible to the Care Insight SCR.

Does Care Insight SCR ensure that these protections do not present a risk to the future safety of the patient?

Patients wishing to opt out of the Care Insight SCR are able to do so by mailed-in form, freephone or by discussing the matter with their GP

Opting out is identified as possibly meaning that clinicians will not have all the necessary information; however the fact that a patient has opted out will be visible to clinical users of the system, prompting them to obtain any necessary information by other means, such as asking the patient.

Does Care Insight SCR address the issue of function creep with regard to intended and possible future uses?

Secondary use of data held on the Care Insight SCR for purposes other than care is explicitly ruled out.

What privacy lessons were learned by the project – how were privacy risks identified and mitigated?

Care Insight SCR is modeled on a Danish system, and was developed with extensive study around the privacy problems discovered and mitigations developed there. A privacy impact assessment was conducted, and the decision not to have a centrally held register of health information and to only provide access to health information after an explicit assurance of patient consent in non-emergency situation were based at least partly on privacy grounds.

Appendix 3: Canterbury eSCR

The Canterbury District Health Board SCR View ("Canterbury eSCR") was developed following the major Christchurch earthquakes of 2010-2011. As a result of the earthquakes, many medical practices lost access to the health information they held about their patients, and many patients presented to hospitals and after-hours clinics without necessary records. There was also a significant residence shift away from affected areas, which existing health information systems were unable to cope with.

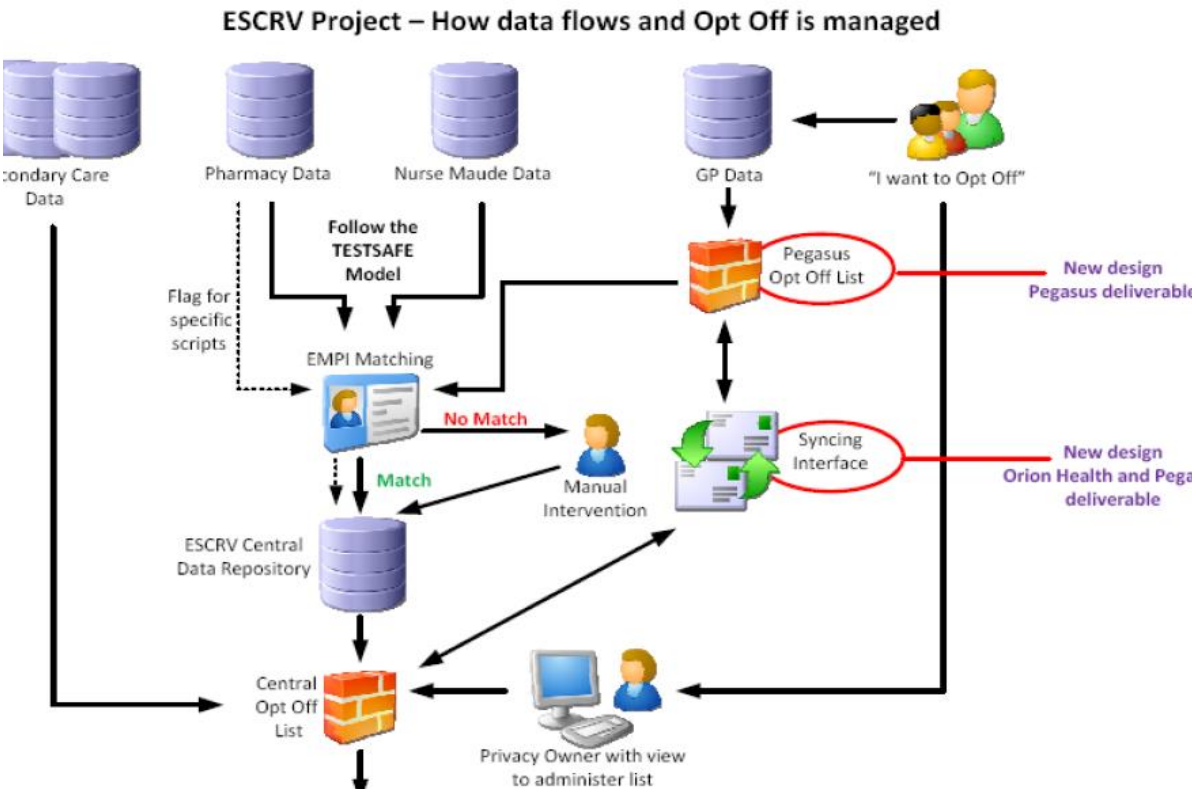
> *There is a comprehensive recovery plan for the Canterbury region and due to the disrupted health system the creation of a eSCRV is an essential strategy of the overall recovery effort. The purpose of the eSCRV is the provision of relevant patient information to health professionals at the point of care so that informed decisions can be made to support the delivery of safe, high quality health care in an efficient way, with the patient being the primary beneficiary. The respectful use of people's health information will be the underpinning principle.*[49]

The Canterbury eSCR creates a shared view of the patient health record by connecting current systems across the Canterbury region, covering around 500,000 people. It is modelled in various aspects on the CareConnect TestSafe system, which began as a regional results repository in the Auckland region before being set up in the South Island.[50]

It works in a way that is comparable to the Compass SCR, with a central repository of clinical data obtained from various sources without explicit patient consent and then filtered. However it has a much wider ambit than the Compass SCR, as it encompasses hospital and pharmacy data as well.[51]

The process for determining whether a given GP has advised his or her patient should be opted off is outlined in the diagram below:

[49] Escrv pia, 2.2 Available at https://healthhub.health.nz/escrv/publicandpatients.html
[50] http://www.careconnect.co.nz/
[51] The platform contains data already collected and held by ERMS (the electronic referral management system) and, at patient level view, TestSafe (lab results) and hospitals. It also includes information held by general practices, community nurses and pharmacies.



Information held on the Canterbury eSCR includes:

- a summary of medical conditions
- details of recent or long-term illnesses
- hospital visits
- operations
- date of last GP visit
- tests and diagnostic results
- medications recently dispensed at community pharmacies
- details about home care visits, including name of the provider and type of care allocated[52]

Around 85% of GPs and 100% of pharmacists in the Canterbury DHB coverage area currently participate in the Canterbury eSCR.

[52] http://www.ssc.govt.nz/sites/all/files/ci-sharedcare-long-2012.pdf

How is Canterbury eSCR populated?

The Canterbury eSCR was set up following a major regional catastrophe that highlighted the pressing need for electronic access to existing health information on a regional basis.

A privacy framework was prepared, based in large part on the Care Connect TestSafe framework.[53] Canterbury DHB also conducted a number of public consultation serminars and a radio campaign, distributed privacy posters and pamphlets to participating clinicians and practices and all households in Canterbury, set up a website and consulted the Office of the Privacy Commissioner.

The privacy framework distinguished itself from a privacy impact assessment, as did its TestSafe equivalent, by restricting itself mainly to operational privacy matters rather than the more policy-oriented analysis that would be normally found in a privacy impact assessment. As such it does not spend a lot of time analysing privacy impacts from the proposed system, but sets out solid privacy protections for the system, including robust opt-off and auditing based on a programmatic assessment ("proximity audit") of whether an accessing clinician was entitled to view a patient's records on any given occasion.[54]

How does Canterbury eSCR demonstrate transparency?

The Canterbury eSCR was developed in eighteen months, from its conception in the aftermath of the February 2011 earthquake to going live in September 2012. Public consultation was carried out by way of a number of public seminars and press releases. The news website Stuff.co.nz featured the project, as did clinical publications. [55]

The relatively brief period of development combined with media interest in stories coming out of the quake-stricken area to make it a popular example of "information-led innovation".[56]

Communications from the project, while waxing enthusiastic about the benefits of the project, were also clear on the process for opting out by calling a free-phone. Brochures and posters were also supplied across the region to all participating clinical venues.

[53] http://www.testsafe.co.nz/downloads/TestSafe_Privacy_Framework_V3-1.pdf
[54] A privacy analysis of the framework including "background, governance, information flows, access to system, legal framewok, purpose, source and accuracy, opt on/off, transparency, security and potential for function creep" was undertaken but is not publicly available.
[55] http://www.scoop.co.nz/stories/GE1110/S00031/canterbury-people-to-benefit-from-health-info-sharing-system.htm
[56] http://www.ssc.govt.nz/sites/all/files/Cab-Paper-Demonstrating-BPS-Christchurch-Innovations.pdf

How does Canterbury eSCR help consumers to maintain control over their own information?

Based on the model of the TestSafe regional results repository, any health consumer may have their health information removed from the Canterbury eSCR. Just as with TestSafe, there is some granularity in the way that opt-offs are handled:

Patients are able to:

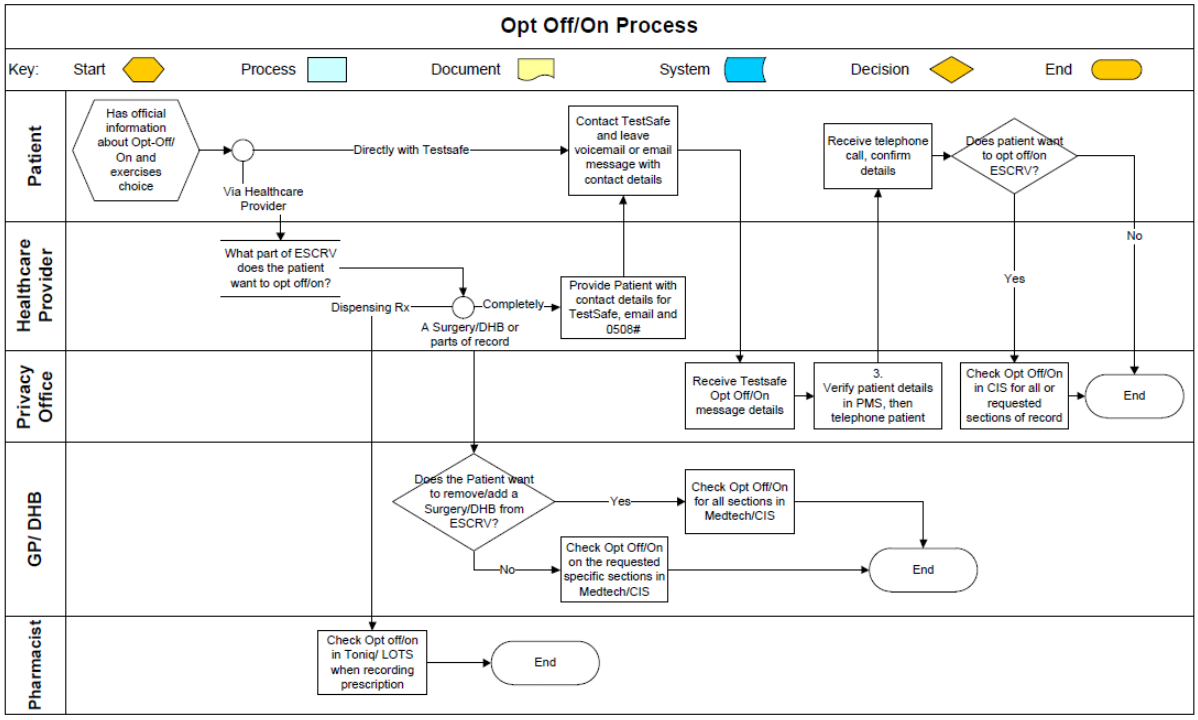
- globally opt off the whole system
- opt off Pharmacy dispensing on a per Pharmacy basis
- opt off from sharing Hospital Data
- opt off from community nursing sharing

At GP Practice the Patients have several options:

- opt out of all Primary Data
- opt out of parts of Clinical Data, e.g. all medications, classifications, etc
- prohibit anything marked 'confidential' from being extracted.[57]

The opt-off process is as follows:

Opt-Off process Flow Diagram



Notes/Assumptions:
1. Healthcare Provider refers to all GP's, Community Nursing, Pharmacists, and Secondary Healthcare Providers incl. DHB
2. Privacy Office to verify patient details on PMS, Homer or SAP
3. Assume GPs can select sections of the GP2GP to opt off and Privacy Office UI has the same capability.
4. Implementation of Opt-off capability requires application developments and is to be delivered in stages

[57] http://www.ithealthboard.health.nz/sites/all/files/NICLG%20-%20eSRCV%20-%20(22-11-12).pdf

How does Canterbury eSCR help consumers to maintain control over their own information?

The Canterbury eSCR also does not mandate the use of the HISF, though its recommendations are generally in line with, or in excess of the Framework. Its privacy framework states that:

> *Existing DHB, Pegasus Health and TestSafe policy applies, in summary this includes:*
>
> - *Privacy Training*
> - *User Identification / Password protocols*
> - *Use of internal and external firewalls*
> - *High availability systems, including backup and recovery facilities*
> - *Audit and monitoring*
> - *Physical security measures*
> - *Mechanisms to ensure the secure transmission of information*[58]

How does Canterbury eSCR protect against function creep?

Under the Canterbury eSCR privacy framework the intended purpose of collection is stated as "to provide relevant patient information to health professionals at the point of care so that informed decisions can be made to support the delivery of safe, high quality health care in an efficient way, with the patient being the primary beneficiary."

The issue of potential function creep is addressed further along in the framework:

> *Over time it is expected that there will be a demand to use the information in eSCRV for purposes other than to treat a patient currently in the care of the accessing health care provider. Broadly, these requests are typically for:*
>
> - *Research*
> - *Health Management*
> - *Health Education*
> - *Service Planning*
>
> *An example where this may occur is to identify patients with a specific condition that are not complying with the standard treatment protocol for that condition.*
>
> *Use of eSCRV for these purposes is explicitly unauthorised under this Privacy Framework Proposal.*[59]

[59] Escrv privacy framework, 5.2.3 Available at https://healthhub.health.nz/escrv/publicandpatients.html

There is also a requirement for further PIA or assessment at governance level before any changes to the purposes for which health information which is intended to mitigate against function creep.

How does Canterbury eSCR govern health information once collected?

Governance of the Canterbury eSCR is provided by the eSCRV Steering Group:

> *The eSCRV Steering Group is responsible for implementing and operating the Privacy Framework. This includes:*
>
> - *Ensuring that the use of eSCRV remains the viewing of relevant information between health providers in different parts of the health sector, for the purpose of enabling and supporting health care delivery.*
> - *Establishing, maintaining and endorsing policies and processes which ensure authorised access to information in eSCRV.*
> - *Considering and resolving issues related to eSCRV information storage or accesses that are raised by audit programs.*
> - *Ensuring that information providers, health care professionals and health care consumers are fully aware of the purposes of eSCRV.*
> - *Ensuring that the eSCRV security processes and functionality adequately support the alliance organisations information access policies and processes, and adhere to best practice security approaches.*
> - *Establishing ongoing eSCRV Privacy Framework Governance post the eSCRV Establishment*

The privacy framework commits the Steering Group to a significant level of detailed analysis of how health professionals are using and accessing the Canterbury eSCR. The eSCR Steering Group reports to a Canterbury Systems Governance Group and is linked to the Information Use and and Management Group for the Canterbury District. Assuming this level of scrutiny is sustained, there is some evidence that improper access to information held on the Canterbury eSCR will be discovered and appropriate steps taken.[60]

Does Canterbury eSCR incorporate sufficiently clear business rules to determine where a justification for disclosure exists?

As with the Compass SCR, access to the Canterbury eSCR is presumed and required to be for the purposes of direct provision of patient care. Ensuring this is the case requires appropriate governance, consistent audit and review and, where necessary, enforcement.

[60] http://www.stuff.co.nz/national/health/8545410/Ryders-medical-files-spied-on

Does Canterbury eSCR take appropriate steps to ensure both clinicians and patients are aware of these rules?

Health practitioners using the eSCR are required to be trained as part of their access to the system, and to sign an Access Deed setting out their obligations and explaining the use of proximity auditing to detect misuse. Brochures and posters describing the Canterbury eSCR are widely distributed, and an appropriately widespread public awareness campaign has been conducted.

Does Canterbury eSCR have appropriate security around the information it holds?

Health information is stored in encrypted form, to a similar level of encryption as the Compass SCR. Access is tracked and logged, and details of access are available on request to patients and practitioners.

Does Canterbury eSCR recognise health information that is of heightened sensitivity for a given patient?

Canterbury eSCR has a confidentiality flag system modelled on TestSafe and allows patient and GPs to designate items and categories of information as confidential with a fair degree of precision, as described above at [ref].

Does Canterbury eSCR address the issue of function creep with regard to intended and possible future uses?

As with Compass SCR, Canterbury eSCR prohibits secondary uses of information it holds.

What privacy lessons were learned by the project – how were privacy risks identified and mitigated?

Canterbury eSCR was developed under pressure to address the health information needs of a region following a major catastrophe. Nonetheless a privacy impact framework was developed that, while not detailed, does cover the key necessary points. As with Care Insight SCR, the privacy and governance processes benefited from being modeled to some extent on an older system, in the case of the Canterbury eSCR the TestSafe privacy framework.

Appendix 4: Definitions

- **Care Insight Server** – a secure, remotely hosted application that allows emergency care staff to submit a web based form requesting patient medical records to connected practices.

- **District Health Board**: Regional health service provision entities that fund all health services in their region (including PHOs). There are currently 20 DHBs in New Zealand.

- **Electronic Health Record:** A full record of care provided to a patient, in electronic form. Able to be used as the primary record of care for clinical purposes.

- **EMR** – the system used for storing electronic patient information and medical history (e.g. Medtech, MyPractice, Incisive). The majority of New Zealand's EMR systems (close to 100%) are already enabled with HealthLink Messaging and are capable of receiving Healthdocs messages and sending back Healthdocs acknowledgements.

- **HealthLink Messaging** – the Care Insight Server is enabled with HealthLink Messaging to allow it to communicate to the EMR (also enabled with HealthLink Messaging) using the Healthdocs standard message. This component is already existing and operational in close to a hundred per cent of New Zealand General Practices.

- **Personal Health Record:** A collection of health information held for, and immediately accessible by, the patient.

- **Primary Health Organisation:** Collectives receiving money from their DHB for providing health care on a capitation basis. In other words, PHOs receive money according to the population they serve. There are currently 81 PHOs in New Zealand.

- **Shared Care Record:** A partial record of care provided to a patient and relevant data to assist collaboration between medical professionals, containing summary clinical and demographic data.