Shared Care Record View
Privacy Framework

Document Control

Document Control			
Compiled By	David McKay, Program Manager, CDHB Michael Furlong, healthAlliance TestSafe Service Manager eSCV Steering Group		
Document History	Revision notes	Version	Release Date
	Review Release	0.1	3 May 2011
	Feedback Updates	0.2	8 May 2011
	Feedback Updates	0.3	6 June 2011
	Feedback Updates	0.4	13 June 2011
	Updates to purpose privacy commissioner office feedback	1.1	15 July 2011
	Updates to purpose wording and branding	1.2	12 August 2011
	Updates to include Pegasus feedback	1.3	2 Sept 2011
	Updates to include revised Opt-Off wording	1.3	29 Nov 2011
Associated Documents	Title	Version	Release Date
	TestSafe Privacy Framework	3.1	Nov 2010
	The Future of Health – Enabled by Information		Nov 2010
Confidentiality	The information contained within this document is proprietary to the Canterbury DHB and healthAlliance Ltd. It may not be used, reproduced, or disclosed to any others except employees who have the need to know for the purpose of this document. Prior to such disclosure, the recipient of this document must obtain the agreement of such employees or other parties who have the appropriate authority to receive and use such information as proprietary and confidential and subject to non-disclosure on the same conditions as set out above. The recipient by retaining and using this document agrees to the above restrictions and shall protect the document and information contained in it from loss, theft and misuse.		

Table of Contents

1. Overview

1.1. Purpose of this document

The purpose of this document is to provide a management summary of the 'Privacy Framework' proposed for the Shared Care Record View ('eSCRV'). Following review and approval processes the document will be used as the basis for the implementing of the privacy framework in accordance with the approach described in the 'Way Forward' section herein. Part of the deliverables of the implementation includes an updated Privacy Framework document suitable for wider publishing.

1.2. Privacy Framework Background

The broad approach proposed for eSCRV is to extend on the TestSafe approach recently adopted in Canterbury for sharing specific information types between primary and secondary care (TestSafe South). TestSafe uses the approach of defining a Privacy Framework to define specifically how DHB privacy policy will be implemented to meet the needs of the various stakeholders.

This differs slightly from a 'Privacy Impact Assessment', the Privacy Commissioner notes:

"The purpose of the assessment is to:

- Identify the potential effects that the proposal may have upon personal privacy
- Examine how any detrimental effects on privacy might be lessened."[1]

The focus of the Privacy Framework is on implementing policy rather than policy development. As eSCRV extends on the TestSafe approach, where appropriate references are made to the current TestSafe Privacy Framework (see 'Associated Documents' above) as the basis of what is described.

[1] Refer to the Privacy Commissioner's website: http://privacy.org.nz/privacy-impact-assessment-handbook/

2. SCV Background

2.1. Purpose for Collection

An overriding principle of the Health Information Privacy Code is to understand the purpose for collecting personal information:

> “Personal information shall not be collected by any agency unless-
>
> (a) The information is collected for a lawful purpose connected with a function or activity of the agency; and
>
> (b) The collection of the information is necessary for that purpose.”[2]

This section describes the background to the eSCRV and how it will be used.

2.2. Purpose of Use

A further requirement of the Health Information Privacy Code is for a health provider to understand the Purpose of Use that would apply when accessing eSCRV information. This is detailed as follows:

> “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 healthcare in an efficient way, with the patient being the primary beneficiary. The respectful use of people’s health information will be the underpinning principle.”

2.3. eSCRV Summary

eSCRV has come about as a matter of urgency following the Christchurch earthquake, with the following underlying principals being identified and agreed:

- Recognition by all that Christchurch is in an emergency
- Recognition that all health services have been substantially affected which will impact for some time creating an extended emergency scenario for healthcare
- Recognition of electronic tool for sharing appropriate information for the benefit of the patient
- Recognition that essential data will be shared by appropriate health professionals with the goal of improving healthcare for patients.

The purpose eSCRV is to create a shared view of the patient record by connecting current systems across the Canterbury Health Care Systems, to ensure and to provide clinical care to the people of the region and mitigate the impact on Secondary Care due to the displacement of services, peoples, clinicians and organisations due to the earthquake.

eSCRV is being established via a project commissioned by a partner alliance between the Canterbury DHB (CDHB) and Pegasus Health, namely eSCRV (Shared Care Record View), and

[2] Health Information Privacy Code: The Information Privacy Principles, Principle 1: Purpose of collection of personal information

is jointly sponsored by David Meates, CDHB Chief Executive Office, and Vince Barry, Pegasus CEO. To meet this urgency the project is modelled on a phased approach based around pilot GP Practices, Pharmacies and Community Nursing users that have been identified by the project followed by ongoing rollout to care providers.

The in-scope systems are CDHB Concerto, TestSafe South, Nurse Maude, General Practices on the Pegasus network, (including Piki Te Ora), using the MedTech32 Practice Management System, and Community Pharmacy using Toniq. Further noting:

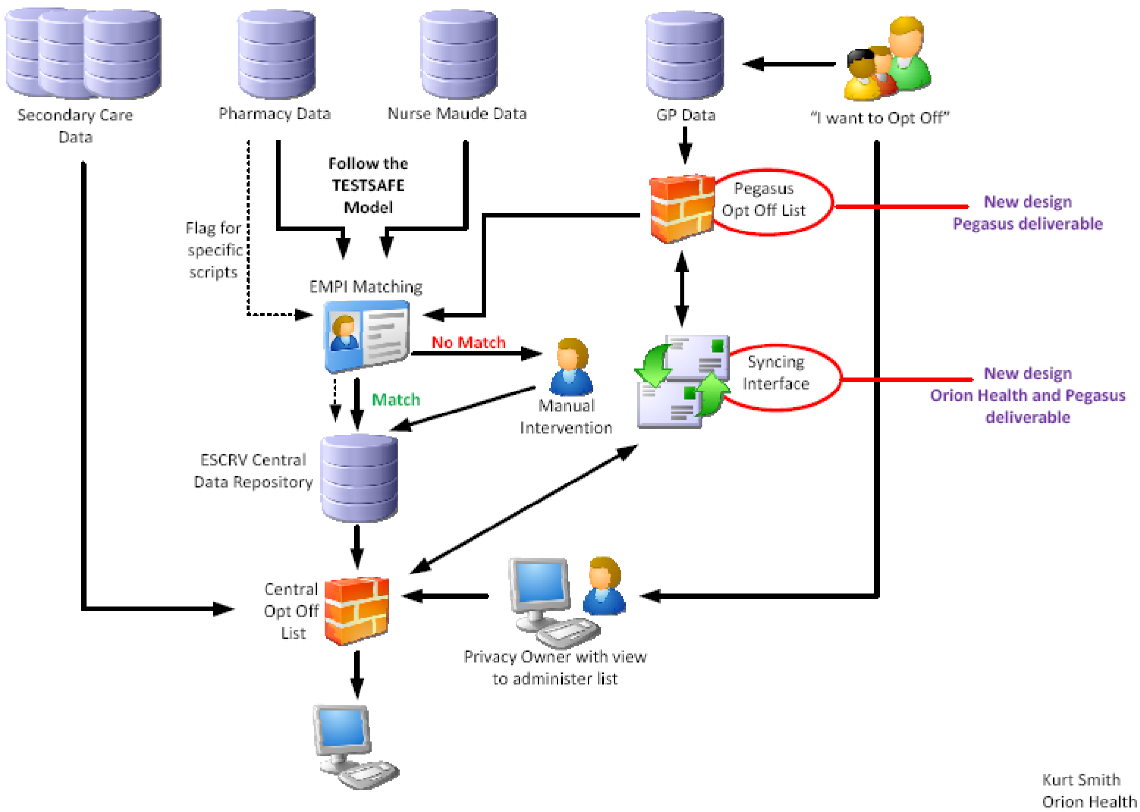
- Record views are being clinically defined across the alliance.
- Dataflow will be GP2GP, CDA and HL7 standards compliant. Noting where this is not possible interim solutions may be utilised and a compliance roadmap agreed.
- The Primary Care CDR (Clinical Data Repository) is to be hosted and supported by Pegasus Health on behalf of the alliance and will include General Practice, Community Pharmacy, and community nursing data sets.
- The eSCRV clinical portal, TestSafe South and Secondary Care CDR are located, delivered and managed by CDHB.
- The Regional rollout will be defined as part of the establishment project.
- Healthcare provider and healthcare consumer privacy materials are to be revised and distributed as part of the enrolment, education and deployment process in accordance with the Testsafe protocol and model.

Operational oversight of the establishment project is provided by the "eSCRV Steering Group" commissioned specifically for this purpose. Governance is provided the "eSCRV Governance Committee" drawn from the alliance and partner executives with a further advisory role provided by the incumbent "CDHB Clinical Information Systems Governance Group". A review of ongoing eSCRV governance requirements and recommendations is a deliverable of the establishment project.

Overall accountability for eSCRV rests with the CDHB CEO and Chief Medical Officer.

A Summary level schematic of how information will be populated into eSCRV is provided as follows. A detailed Opt-Off process flow is attached as appendix 1 to this document.

ESCRV Project – How data flows and Opt Off is managed


Secondary Care Data
Pharmacy Data
Nurse Maude Data
GP Data
"I want to Opt Off"
Follow the TESTSAFE Model
Flag for specific scripts
Pegasus Opt Off List
New design Pegasus deliverable
EMPI Matching
No Match
Match
Manual Intervention
Syncing Interface
New design Orion Health and Pegasus deliverable
ESCRV Central Data Repository
Central Opt Off List
Privacy Owner with view to administer list

Kurt Smith
Orion Health Ltd

3. Governance

eSCRV Governance Committee

The eSCRV Governance Committee membership includes:

- CDHB; David Meates, Chief Executive Officer
- CDHB; Nigel Millar, Chief Medical Officer
- Nurse Maude; Jim Magee, Chief Executive Officer
- Pegasus Health; Martin Seers, Chairman
- Pegasus Health; Martin Wilson, GP Liaison Group
- Canterbury Community Pharmacy; Peter Fear
- Pegasus Health; Vince Barry, Chief Executive Officer

eSCRV Steering Group

The SCV Establishment Steering Committee membership includes:

- CDHB; Chief Medical Officer.
- CDHB; CIO.
- Nurse Maude; Director of Nursing.
- Orion Health; New Zealand Manager.
- Pegasus Health; Business Information Services Manager / Privacy Officer.
- Pegasus Health; GP / Clinical Leader – I.T.

  Canterbury Community Pharmacy 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 healthcare 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, healthcare professionals and healthcare 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 project.

Advisory Groups

The eSCRV Steering Group will, at its discretion, seek feedback from appropriate ‘advisory groups’ to ensure decision making is robust and can withstand subsequent stakeholder review. Advisory Groups include, but are not limited to:

- CDHB, Nurse Maude, Orion Health and Pegasus legal expertise.
- CDHB, Nurse Maude, Orion Health and Pegasus Privacy Officers and expertise.
- Nurse Maude Clinical and Healthcare consumer Advisory Group(s).
- Pegasus Healthcare Consumer, GP and Pharmacy Advisory Group(s).
- Privacy Commissioners Office
- NHIB Consumer Group

4. HIPC Summary

This section sets out the way in which eSCRV information will be managed in the context of the Health Information Privacy Code.

HIPC Principle	Summary of Implementation approach	
1. Purpose of collection.	▪ Refer to previous section '2 SCV Background'	
2. Source of information.	*Primary Care Information Sources*	*Primary Care New Practices*
	▪ Pegasus Medtech32 GP Practice Management Systems.	▪ Selected information (with NHI) sent to eSCRV Primary Care CDR and viewed via eSCRV Service.
	▪ Toniq and Lots Pharmacy Dispensary Systems.	▪ All prescribed dispensing (with NHI) sent to eSCRV Primary Care CDR and viewed via eSCRV Service.
	▪ Laboratory test results (TestSafe South)	
	▪ Allied Health, Nurse Maude.	▪ Selected information (with NHI) sent to eSCRV Primary Care and viewed via eSCRV Service.
	Secondary Care Information Sources	*Secondary Care New Practices*
	▪ Inpatient systems.	▪ Summary encounter information view via eSCRV Service.
	▪ Laboratory Results (Testsafe South).	▪ Results view via eSCRV Service.
	▪ Outpatient systems.	▪ Summary visit information view via eSCRV Service.
3. Collection of information from individuals.	▪ Refer to TestSafe Privacy Framework, Section 3.3, the same approach will be adopted, i.e. patient notification based, not consent based. ▪ The model will be extended to be applied to secondary care also in reflection of the sources of Information noted above, i.e. Patient Notification (Posters & leaflets), and Patient Choice (Opt-Off), Refer appendix 2 '*Testsafe Privacy Framework.*	
4. Manner of collection.	▪ Existing policy applies, i.e., the manner of collection will not be altered by eSCRV. As for any collection of information, the healthcare professional that is collecting the information from the individual must do so in a sensitive and private manner.	
5. Storage and security.	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 (refer to the "Section 5.eSCRV Privacy Features). ▪ Physical security measures. ▪ Mechanisms to ensure the secure transmission of information.	

HIPC Principle	Summary of Implementation approach
6. Access to personal health information.	Existing eSCRV partner organisation policy applies. In summary, if a health consumer wishes to access such information, requests should be transferred to the CDHB Privacy Officer service which will liaise and process that request in accordance with the source organisations policy and processes.
7. Correction of information.	The healthcare consumers request will be transferred to the healthcare provider managing the systems from which the information was sourced. It is then the responsibility of that provider to correct the information or attach a statement setting out the correction sought but not made, in line with their existing policy and processes. Corrections and statements of correction will then be published to the eSCRV via implemented processes.
8. Ensuring accuracy before use.	Existing eSCRV partner organisation policy and processes applies. In summary: ▪ Healthcare providers contributing information are to ensure information is accurate in accordance with their policy and process. ▪ The history of updating records is to be auditable, including the date and time records were sent and / or updated.
9. Retention of Information.	Existing DHB, Pegasus Health and TestSafe policy applies; i.e. the minimum retention period for records is to be 10 years or any longer period specified under the DHB's General Disposal Authority (via the Public Records Act 2005.
10/11. Limits on use and disclosure of information.	▪ Existing DHB policy and processes applies for providing eSCRV access to DHB staff, where necessary policy documentation is to be updated to include reference to eSCRV. ▪ eSCRV partner organisation access is to be provided only to authorised healthcare professionals who's registration can be verified via the health practitioner Index provided by the Ministry of Health. ▪ An option is provided to patients to restrict the sharing of their information, refer Section 5 eSCRV Privacy Features .
12. Unique identifiers.	eSCRV is to use the unique NHI number assigned to each healthcare consumer as an identifier. This is consistent with both current sector standards and is necessary for the purpose of data matching / creating of record views within eSCRV.

5. eSCRV Privacy Features

The primary distinction between the eSCRV approach, by comparison to the previous situation of 'islands of information', is that:

> Healthcare professionals may view (parts of) healthcare consumer ("patient") records without the need to seek (source) them directly from the healthcare providers that collected the information from the healthcare consumer.

Consultation conducted by the National Health IT Board (2010) found that in general patients are 'overwhelmingly positive'[3] about sharing health records for the purposes prescribed by eSCRV. However there are a number of common concerns that need to be addressed, these are summarised as the following 'key themes'[4]:

> "Special sensitivity of some information.
>
> Access and audit of access by healthcare providers "

The specific features of the Privacy Framework to address these concerns are detailed below. These are based on an extension of the TestSafe approach which includes a number of practical measures and lessoned learned developed over time.

5.1. Healthcare Consumer ("Patient") Choice

The ability for patient to choose to share their information via eSCRV is a key element to the overall approach. This implements the principle that the patient is the only person who can decide if information has 'special sensitivity' and should therefore not be shared. It is important to note that this is not a choice for the information to be collected[5], only a choice as to how the information is shared.

5.1.1. eSCRV Implementation Approach

Patients may only choose to prevent their record sharing via the eSCRV (referred to as Opt-Off), i.e. they can:

- Prevent primary care based healthcare providers from viewing records sourced from secondary care (and other primary care providers).
- Prevent secondary care based healthcare providers from viewing records sourced from primary care.

Patients may not restrict access to information within the collecting healthcare provider's organisation.

- Only the viewing of the new 'flow of information' between healthcare providers may be restricted.
- DHB based facilities are considered to be a single 'organisation' regardless of the fact that there are multiple physical locations and / or departments for healthcare delivery[6]. Further noting this relates to all participating regional DHB.

[3] National Health IT Board, 'The Future of Health – Enabled by Information', Workshop Outcomes

[4] National Health IT Board, 'The Future of Health – Enabled by Information', Key Themes. NOTE: The theme of 'Permission' is addressed by existing policy, refer to Section 4, HIPC Summary, Principle 6. Access to personal health information.

[5] Refer to section 4 HIPC Summary, Principle 3.

[6] This aspect will be considered further in the HealthCare Consumer consultation planned, refer to '4 HIPC Summary' following.

- Where viewing is by healthcare professionals with a dual appointment, i.e. they have a role in both primary care and secondary care, the viewing must be under the rights of the organisation providing access, they may not exercise the viewing / access rights provided by their other role unless consent is explicating requested from the patient.

5.1.2. Restricted Information Viewing Levels (Opt-Off)

Restricted information viewing is to be provided at the following levels:

- Patient Level i.e.; all clinical data captured for use in eSCRV will no longer be viewable except in the source system. Further noting;

  a) The TestSafe South (Pharmacy and Laboratory) application opt-off flag (if set) will be honoured i.e.; if the patient chooses to opt-off a script or laboratory result eSCRV will not display this, even if at patient level the patient has not opted off.

  b) The GP provider for presumptively sensitive information can at their discretion or at the explicit instruction of the patient prevent the information from being captured for use in eSCRV

- Restricted information view for date range:

  a) This allows restriction to be confined to specific ‘encounter’.

  b) A primary care example is: restriction of sharing information with secondary care for the date associated with a visit to specialised clinic or test.

  c) A secondary care example is: restriction of sharing information with primary care for the date of a specific inpatient/day stay event.

Information viewing restriction indicated:

- If the GP Provider has chosen discretion or at the explicit instruction of the patient to prevent information from being captured for use in eSCRV, there will not be an indication that this is the case highlighted to the healthcare provider accessing eSCRV.

- If the patient has chosen to prevent viewing information, an indication that this is the case will be highlighted to the healthcare provider accessing eSCRV.
- The nature of the information prevented from being viewed will not be indicated.
- This maintains the patients wish for confidentiality whilst providing a prompt to the treating health professional to seek further information from the patient if it could be clinically relevant. This allows the patient to effectively control the viewing of sensitive information depending on the circumstances.

Option to remove information viewing restrictions:

- For a number of unforeseen reasons, patients may wish to allow viewing of information previously restricted. The system will allow for this in a manner that keeps a history of when the viewing restrictions where applied and removed.

5.1.3. Health Consumer (“Patient”) Communications”)

Patients’ choice is only effective as a measure to address their concerns if they are aware of their options. The following communications will be provided to meet this requirement:[7]

[7] See also, TestSafe Privacy Framework, Section 3.3 ‘Collection of Information from Individuals’, ‘Advice to Patients’ pg 15

Posters:

- These are to be displayed at ‘intake’ areas in primary and secondary care facilities. The CDHB Privacy officer will undertake regular ‘sample’ audits to ensure / monitor compliance.
- Information will be summary in nature, directing the patient to the other sources of information (noted below) for more detailed information.

Patient Information sheets:

- These will be in the form of pads with tear off sheets which will be distributed to ‘intake’ areas in primary care and enrollment/triage areas in secondary care facilities.
- Provide more detailed information on HealthHUB, including translations.

eSCRV Website

- This includes FAQs and other information for healthcare providers as well as patients.

Free Call Telephone:

- Patients may call toll free 0800 or 0508 number. This will reach the CDHB Privacy Officer who will be briefed on how to respond to patient queries. A key reference for the call centre is the eSCRV website.

Selected Printed Forms:

- A brief message will be included on selected forms produced in patient encounters / visits with healthcare providers. Currently this includes; Laboratory Order forms from GP PMS systems and Receipts from Pharmacy Dispensary systems.

Media Promotion:

- Media releases will be made regarding the eSCRV at the time of its implementation in accordance with the agreed eSCRV Establishment Project communications plan.

5.2. Access Control

The primary purpose of eSCRV is to support healthcare providers delivering care to the people of the region and mitigate the impact on Secondary Care due to the displacement of services, peoples, clinicians and organisations due to the earthquake.

Controls on viewing patient records and review of the use of this viewing are to be put in place to support this requirement. The latter aspect is covered in the next section 'Audit of Viewing'. Over time it is expected that there will be a demand to use the information collected for purposes other than direct delivery of care to patients. Use of eSCRV for these purposes is explicitly unauthorised under this Privacy Framework Proposal.

Specific arrangements are established at the outset for this to ensure patient concerns are managed in the future. This is detailed in Section 5.2.3 "Access requests not related to direct patient care".

5.2.1. eSCRV Implementation Approach

Primary Care eSCRV access is to be provided under the following conditions:

- To authorised healthcare professionals who's registration can be verified via the Health practitioner Index provided by the Ministry of Health.
- To authorised partner organisations Administration, Information Technology and Technical personal executing their responsibilities as prescribed by their employee contracts and roles.
- Healthcare professionals must sign an 'Access Deed' confirming their obligations to use eSCRV for its intended purpose and willingness to comply with patient communications, audit and review procedures.
- Via a secure Health network, e.g. SafeCom, DHBOO, Pegasus Wide Area Network (WAN) or networks as authorised by eSCRV Governance and direct (firewalled) connection between DHB's and Pegasus Health.
- GP viewing will be in patient context provided via GP PMS integration (e.g. Medtech32) and secure URL.
- Community Nursing and Pharmacies viewing will be provided via IE Browser interface.
- Audit checks are to be performed after the patient record has been viewed to determine if there is a 'prima facie' reason for the viewing (see next section ' Audit of Use').

Secondary Care eSCRV access is to be provided under the following conditions:

- Existing DHB policy and protocols for health professional identification and password security apply.
- Via secure DHB networks or secure health network (not public networks / internet).
- Obligations regarding patient privacy are detailed in Employment Agreements.
- Specific 'Confidentiality' agreements regarding the use of health consumer information.
- Ongoing training regarding these obligations.

5.2.2. Consent to View

As noted under section 5.1.2 "Health Consumer ("Patient") Communication" patients choice is only effective as a measure to address their concerns if they are aware of their options. Health professionals are therefore to advise and request consent from a patient prior to accessing eSCRV GP information. A mechanism to record that this has occurred is to be implemented e.g. pop up text screen with default options 'patient consent provided'.

However there maybe a variety of circumstances where a healthcare provider may wish to access GP information without, or prior to, patient consent to view being provided. There is widespread support for the "break glass" (BTG) concept where a clinician could gain access to view a Shared Health Record view and justify the decision later. While eSCRV will not implement BTG which is reliant on establishing a GP to Patient relationship it will utilise the challenge recording mechanism as described above and Event Proximity Audit, refer Section 5.3.2, when viewing patient GP information under these circumstances.

5.2.3. Access requests not related to direct patient care

As noted above, 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 healthcare 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.

It is however further noted that there maybe occasions where requests for information maybe made. In all instances these requests will be transferred to the agency that provided the information and will be executed in accordance with their policy and procedures. Examples are included below, however patient and provider identifiable data is explicitly excluded for Research, Health Service Management, Service planning, and Health Education.

- Legally obligated, e.g. search warrants, court order
- Legally permissible, e.g. CYF (Child Youth and Family), Police under s22C Health Act

5.3. Audit of Use

The purpose of audit is to verify that that eSCRV is used for its intended purpose, i.e. to support a healthcare provider engaged in delivering care to the people of the region and mitigate the impact on Secondary Care due to the displacement of services, peoples, clinicians and organisations due to the earthquake. Three types of audit for eSCRV will be established, these are described below.

5.3.1. Patient Requested Audit

- A patient may request a report of who has viewed their eSCRV records at any time.
- The request may be lodged by calling the free-call number (supported by the DHB Patient Information Office / Privacy Officer) or by contacting the DHB Patient Information Office.
- The report must be picked up by the patient from the DHB Patient Information Office / Privacy Office who will verify identity prior to providing the information.
- The report will include the names, designation and date of access of the different health providers, administrators, information technology and technical staff viewing the patients record.

5.3.2. Event Proximity Audit

- All data presented to eSCRV will include an identifier for the 'collecting organisation'.
- All health professional access to eSCRV, or their eSCRV identity, will be able to be related to an 'accessing organisation'.
- Automated and manual processes will be established to identify the viewing of a patients record where the health professional 'accessing organisation' does match any recent (past and future) records provided by 'collecting organisations'.

  For example:

  Dr Smith accesses Patient X on 1/8/2011. Dr Smith is linked to the Good Guys General Practice. Proximity Audit performs a check to confirm that there are records in eSCRV from the Good Guys practice for Patient X on 1/7/2011. No 'Review' record is created.

  In the above scenario, if there was no record in eSCRV from the Good Guys practice (in the agreed timeframe). A Review record would be created.

  Review records are then sampled and a letter based 'please explain' process is invoked to seek feedback from the health professional as to the context in which they viewed the health consumers records.

5.3.3. Improper Use

Following the completion of a Please Explain process that has identified an improper use of eSCRV, the following actions may be undertaken:

- A formal warning to the health professional of their agreed responsibilities to manage patient privacy and meet eSCRV obligations.
- Removal of the health professional access to the eSCRV.
- Advise of the Improper User of the eSCRV to the healthcare provider's registration authority and/or the Office of the Privacy Commissioner.

Further noting:

Initially eSCRV Steering Group instructions will be sought as to the appropriate level of action and over time escalation procedures will be formalised and documented.

6. Approvals

6.1. Endorsements

Date

Date

Date

Date

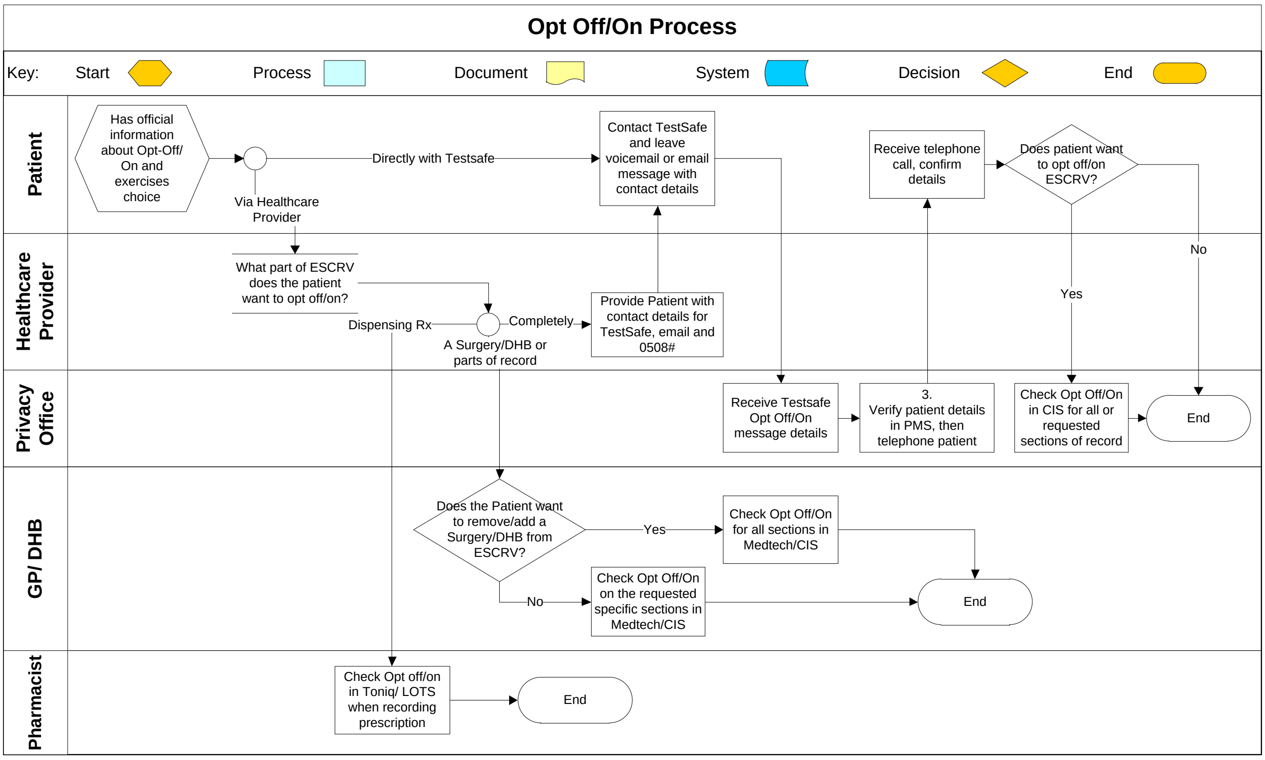
6.2. Authorisation

Date

Date

Appendix 1

Opt-Off process Flow Diagram


Opt Off/On Process
Key:
Start
Process
Document
System
Decision
End
Patient
Healthcare Provider
Privacy Office
GP/ DHB
Pharmacist
Has official information about Opt-Off/ On and exercises choice
Directly with Testsafe
Contact TestSafe and leave voicemail or email message with contact details
Via Healthcare Provider
Receive telephone call, confirm details
Does patient want to opt off/on ESCRV?
No
Yes
What part of ESCRV does the patient want to opt off/on?
Dispensing Rx
Completely
A Surgery/DHB or parts of record
Provide Patient with contact details for TestSafe, email and 0508#
Receive Testsafe Opt Off/On message details
3. Verify patient details in PMS, then telephone patient
Check Opt Off/On in CIS for all or requested sections of record
End
Does the Patient want to remove/add a Surgery/DHB from ESCRV?
Yes
Check Opt Off/On for all sections in Medtech/CIS
No
Check Opt Off/On on the requested specific sections in Medtech/CIS
End
Check Opt off/on in Toniq/ LOTS when recording prescription
End

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

Appendix 2

TestSafe Privacy Framework

TestSafe_Privacy_Fr
amework_V3-1.pdf