National Health Shared Care Plan Programme
Together we can achieve more

Privacy Overview

Introduction

This document provides an overview on the package of measures put in place to manage patient's privacy and confidentiality for the National Shared Care Plan Programme ('NSCP').

The NSCP was formed to initiate pilot projects which trial approaches to shared care to support long-term condition management. The northern region DHB's information services organisation, healthAlliance, is engaged by the National Health IT Board to manage the programme.

The detailed approach to managing patient privacy is available in a document referred to as the Privacy Impact Assessment ('PIA'). This is a summary of the PIA which was developed with input from a number of stakeholder and management groups, these are summarised under the heading 'Governance' below. In addition to these groups, the Privacy Impact Assessment has been reviewed by the office of the Privacy Commissioner.

NSCP Privacy Approach Summary

The privacy approach can be summarised as a package of measures in four areas:

- Patient and Provider Agreement
- Systems and security
- Monitoring access to records
- Governance.

Patient and Provider Agreement

An overarching aspect to the NSCP pilot privacy approach is formal agreement by both the patient and health care providers involved.

All patients participating in the programme undertake an ethics approved, informed consent process. This explains how their information is collected and used and forms the basis for the underlying systems and procedures to operate.

Community based healthcare providers participating in the NSCP are required to read and sign an Access Deed. The deed details standard obligations regarding the management of patient privacy and establishes User acceptance of system access audit processes. Only registered healthcare professionals may be granted access and their registration is checked before login is allocated. This ensures only health providers that work to a code of conduct and privacy of patient information, may see a patients record. DHB based users are subject to standard DHB policy, which includes signed confidentiality agreements and appropriate clauses in employment contracts.

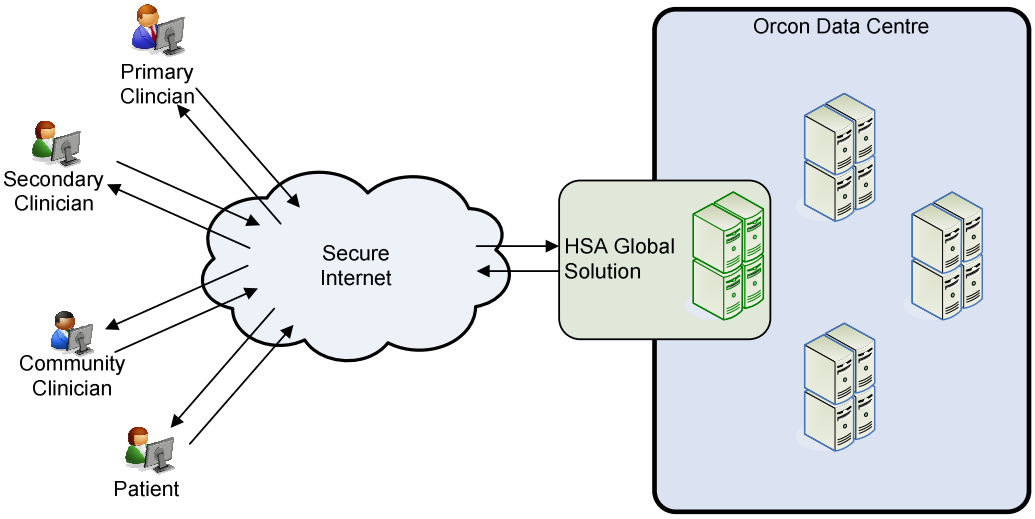
Systems and security

The underlying system used is for the NSCP pilot projects is known as Collaborative Care Management Solution ('CCMS') and is provided by Health Software Anywhere Global ('HSAG'). In summary, CCMS allows different health care providers, and the patient, to interact using an electronic shared care planning tool

It is important to note that this includes:

- a 'patient portal' that patients will be able to login to view their information.
- a 'snapshot summary' available to clinicians in DHB based facilities (e.g. hospitals, outpatient clinics).

HSA Global's CCMS application is a web-based solution. It is delivered via web browsers to patients and community health care providers, and as a web application within existing clinical applications, for primary and secondary health care providers. Data is sent and received via secure secure internet connections to the Orcon Data Centre in Northcote, Auckland. 'Secure Internet' being encrypted https (TLS 1.2) internet connections to the secure data centre.



Orcon host the servers owned by HSAG to deliver the CCMS application and store data. HSAG controls what software and data is on those servers and who can access it. Orcon and their staff cannot access applications or data or move data to other locations inside or outside New Zealand. Orcon provides a sophisticated facility with industry standard measures to support high availability and security:

- 24-hour surveillance
- Monitored alarms
- Swipe card access only
- Secured and re-enforced doors and windows
- Security Policy
- Customer Equipment Policy
- Raised Floor
- Double-layer concrete walls
- Concrete pole building supports

Monitoring Access

Controls are in place to monitor who is part of the care team for a patient and who has accessed their records. Care team members may be nominated by the care team coordinator (usually a GP) or seek access in certain circumstances such as:

- they are a treating clinician
- they have received permission from the care coordinator
- they have received permission from patient.

All access, by members of a care team, or by a secondary clinician to the snapshot summary, is tracked by CCMS. This information is available to patients who can perform 'patient centered audit'.

Patient centered audit involves the patient reviewing the log of who has accessed their records over time. Rather than looking at access to records from the perspective of health care providers, the approach is focused on what activity has occurred, in general, for a particular patient. Patients may request access to the NSCP "Patient Portal". This is an internet based service which includes a detailed log of who has accessed their NSCP record. In addition, an access log may be sent to a selected sample of patients. In both cases the patients can verify for themselves that all accesses have been appropriate.

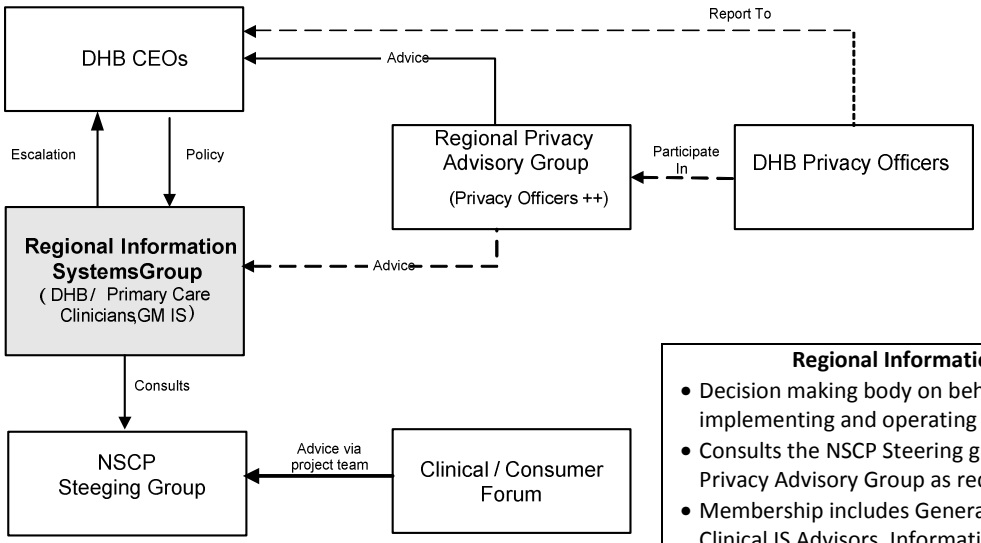
Improper Use

If, for any reason, the appropriateness of access is questioned, the healthcare provider concerned may be contacted by the NSCP service to provide explanation. Following the completion of a 'Please Explain' process that has identified an improper use of NSCP, the following actions may be undertaken:

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

Governance

In a legal sense, the obligations to manage privacy lie with the agency collecting and storing the information. In this context this is the DHBs, via healthAlliance, who in turn has contracted a vendor. The DHBs body for governing the privacy matters for regional information systems is RISG ('Regional Information Systems Group. The groups involved, their roles and representation is summarised below:



Regional Information Systems Group (RISG) • Decision making body on behalf of the DHBs, responsible for implementing and operating the Privacy Framework. • Consults the NSCP Steering group and seeks advice from Regional Privacy Advisory Group as required. • Membership includes General Manager Information Systems, Clinical IS Advisors, Information Managers and GPs (performing a primary care liaison role).
NSCP Steering Group • Governing body for the programme, makes recommendations to RISG. • Representation includes consumers and a rang of primary and secondary care clincians.
Regional Privacy Advisory Group (RPAG) • DHB based advisory group, including legal expertise. • Representation includes General Practice.
Clinical – Consumer Forum • Independent advisory body to the NSCP including healthcare professionals and consumers.