Orion Shared Care Platform Privacy Impact Assessment

Document Approval

Approver	Date	Signature
Tim Marsh, NNSW LHD Orion Project PM	January 9th 2017	[SIGNED]
Matt Long, NNSW LHD CIO	January 18th 2017	[SIGNED]
Vicki Rose, NNSW LHD Executive Director Allied, Chronic and Primary Care	January 18th 2017	[SIGNED]

1 Executive Summary

The Orion Shared Care project will deliver a fit-for-purpose, customised, electronic shared care planning and secure communication tool to the NSW North Coast.

The Orion Health Shared Care Platform is being developed for the purpose of facilitating treatment and ongoing care of chronic and complex care patients, most specifically, “integrated care patients”.

It facilitates communication and information gathering in a responsible, ethical and legal manner, for the purposes of shared care planning and management of patients.

It involves end users from Primary Care (GPs, Practice Managers and Practice Nurses), the NNSW Local Health District and Private Service Providers.

Since it will collect Private Health Information (“PHI”), a Privacy Impact Assessment (“PIA”) is recommended for completion by the NSW Privacy Commissioner and Office of the Australian Information Commissioner (“OAIC”).

This PIA is focussed on privacy protection for patients. Privacy of users of the system—limited to collection of name and email—is handled via a Privacy Policy for system users (link).

A Privacy Threshold Assessment (“PTA”, [2]) which informs whether a PIA ought to be completed confirmed that a PIA was warranted.

This document is that PIA.

There is currently no obligation to complete a PIA, but completion of a PIA confers rigour and quality to the project so is seen as a critical aspect in addressing the privacy obligations of the project.

The purpose of this Privacy Impact Assessment (PIA) is to future-proof the Orion Shared Care Platform for potential endorsement across all of NSW Health by ensuring the system, and project approach, complies with relevant privacy legislation and privacy best-practice.

Key personnel from the NNSW LHD, eHealth, GPs and to some extent NSW Health Legal Branch have been involved in the development of Orion and particularly the privacy and access regime.

Key design considerations were identified to protect patient’s right to privacy and security of their heath record information as per legislation.

This assessment has adjudged the privacy risk due to the Orion Shared Care system as low.

A list of recommended actions to address identified privacy risks are below. They are contained in Table 14.

The risk of not implementing recommendations varies depending on the recommendation. Therefore the risk to the Project Board, and more broadly the LHD Executive, is dependent on which recommendations are accepted for implementation.

However, recommendations are consistent with ensuring information and privacy is protected in accordance with the relevant Acts, and that the privacy framework is consistent with Australian Privacy Principles.

Therefore, in general, the risk to the Board and Executives in not implementing is similar to other systems and projects not in compliance with privacy best-practice.

All recommendations should be considered for adoption. Most do not confer any cost on the LHD, as they can be actioned under existing policies and frameworks. The exceptions to this statement relate to recommendations 18, 23 and 32. For these recommendations, a proposal for management of risk, whilst minimising cost, is made.

1. Address privacy breaches in training, and by adding information for system users to privacy page.
2. Add general web/app privacy policy for web/system use and APP-compliant patient privacy policy.
3. Make sure links to privacy policy are in brochures.
4. Make the privacy policies downloadable in PDF format on the website.
5. Seek advice on privacy breach handling procedure: should the system be subjected to existing frameworks, or have a new process.
6. Engage consumer representatives in any further privacy changes, using existing processes and forums.
7. Seek clarification on whether IHIs are collected and used in accordance the Healthcare Identifiers Act and Healthcare Identifiers Regulation 2010. [Completed – 5/12/16]
8. As much as possible, funnel all support requests primarily via the webpage (hosted in Australia). These forms can have PHI stripped out before being sent to the Helpdesk to manage ticketing.
9. Educate users not to enter PHI and unsolicited information into contact/helpdesk forms.
10. Use checkboxes (required) on forms on the website and helpdesk that the user will need to check to confirm they are not entering PHI.
11. Seek to have the Integrated Care website served entirely over SSL.
12. Seek review of the Patient Information and Privacy Pamphlet.
13. [Use] That secondary use cannot be declined as it would result in creation of a declined-secondary-use register (with IHI), which a) it is in and of itself a risk, b) is a non-trivial amount of work to implement and c) the privacy risk from secondary use[1] is minimal and proportional to use.
14. Seek advice on whether the notification period for changed privacy policy (potentially 9 months or more), is too long. If so, seek advice on how to notify patients of policy change.
15. Seek legal advice on whether IHI suppression is needed from the system or on forms intended for print. IHIs are used to uniquely identify patients.
16. That a select number of records be collected after a period of operation, and at planned intervals, and be analysed for quality.
17. That GP and end user training cover off information quality obligations, particularly for GPs.

[1] “Secondary Use” is defined as any purpose other than the primary purpose for which the APP entity collected the personal information. For example internal business practice such as reporting, auditing or benchmarking.

18. Recommended that an annual audit function (at a minimum) and resource be approved. Health policy states: System/Application administrator should monitor the event logs created by the system/application to ensure that inappropriate behaviour or potential intrusions are recognised and addressed. Audit log should be examined at a minimum every fourteen (14) days. The responsibilities should be formally assigned and documented in operational management procedure. Given that this project is a Proof of Concept, it’s proposed that this be adopted if the project is scaled beyond the 12 months. Moreover, it’s proposed that this be facilitated under existing procedures, frameworks and resourcing.
19. Seek advice on current IT system data breach processes.
20. That a record delete (expunge) function be requested of Orion post 12 months, in accordance with below recommendation.
21. Seek advice on whether a patient request for removal of their record from the system comports with Corporate Records Act requirements for retention.
22. Redacted – retention in accordance with Corporate Records Act. Seek advice on whether an information retention and destruction policy needs implementation or if existing policies can be applied.
23. That a review period for the PIA and related policies and processes be agreed, funded, resources and conducted. This includes review of purpose, use, collection and annual system use audits, as well as destruction. Given that this project is a Proof of Concept, it’s proposed that this be adopted if the project is scaled beyond the 12 months. Moreover, it’s proposed that this be facilitated under existing procedures, frameworks and resourcing where possible.
24. Seek advice on how to ensure non-LHD users are subject to minimum IT standards (inferred through Privacy Act and HRIP Act). Potentially use MOU or signed Ts and Cs.
25. That advice is sought on how patients should request access to their information held in Orion: use existing practices, or create an Orion-specific process. A request form may need to be added to the Orion project website. This information/process needs to be highlighted on the Orion project website, in the privacy section. Patient information policy: access, corrections, destruction, complaints.
26. That advice is sought on how patients should request access or request corrections to their information held in Orion: use existing practices, or create an Orion-specific process. A request form may need to be added to the Orion project website. This information/process needs to be highlighted on the Orion project website, in the privacy section. Patient information policy: access, corrections, destruction, complaints.
27. Seek advice on whether the system be subject to current information management policies.
28. Seek advice on who “owns” the system from a governance (information custodianship and accountability) perspective.
29. Seek advice on how subpoena requests ought be managed.
30. Seek advice on advising Medical Records of the existence of the system so that the system could be interrogated by Records in the event of a subpoena.
31. Ensure training covers off access, corrections, destruction, complaints as well as privacy obligations, or that the information is on the website at a minimum.
32. Subjecting the PIA, PIA response and PIA review to independent review such as the OAIC or NSW MOH Legal or NSW Government Legal. It is suggested that the Ministry of Health Legal and/or Privacy departments may sufficiently satisfy the “independent” test, and minimise cost in providing such review, for the purposes of the time-limited Proof of Concept. The Project Board and indeed LHD executive may view it prudent to engage an independent 3rd party review of the PIA in the event that the project is extended for wider use.

Document Control

Document Version

Version:	1.0
Date:	9 Jan 2017
Status:	Version 1 for Approval
Document number	TBA
Location	W:\IntegratedCare\Operations\TIMS OLD FOLDER\ICP\SCP\Orion POC\privacy\NNSW Orion PIA v1.0.docx

Distribution List

Name	Title	Date	Version
J. Hathaway **D. Goldie** **C. Wilson**	Privacy Manager Emergency Department Nurse Unit Manager (NUM)IC Manager	29/11/16	0.1
M. Long	CIO	7/12/2016	0.2
M. Long	CIO	9/1/2017	1

Document History

Version Number	Version Date	Description
0.1	21/11/2016	Draft v0.1 WIP
0.2	02/12/2016	Incorporate J. Hathaway's comments.
1	9/1/2017	Incorporate M. Long's comments and issue for approval

Documents with revision numbers in the format X.xx, where xx is not zero, are part of the review cycle. e.g. 0.2 is the second draft for review. Documents where xx is zero are final versions which have been approved and are no longer in the review cycle. e.g. 1.0 is a final version

Table of Contents

Figures

Tables

2 Abbreviations and Acronyms

Abbreviation/Acronym	Meaning
APP	Australian Privacy Principle (derived from Privacy Act)
EMR	Electronic Medical Record
NNSW	Northern NSW
OAIC	Office of the Australian Information Commissioner
PHN	Primary Health Network
PIA	Privacy Impact Assessment
PMS	(GP) Practice Management System/software
PTA	Privacy Threshold Assessment
POC	Proof of Concept
SCP	Shared Care Planning (process and system)

3 Related Documents

Ref #	Document ID	Title	Location
1		Project Initiation Document	SharePoint
2		Privacy Threshold Assessment	Sharepoint
3		Privacy Impact Assessment Guide (NSW Privacy Commissioner)	Sharepoint
4			
5			
6			

4 Terms and meanings

Terms and meanings, such as "reasonable" and "reasonably" are held to their ordinary meaning, further explained in Australian Privacy Principles (APP) Key concepts[2] (link).

Meanings without definition in the Privacy Act are used in accordance with their definition in the APP Key concepts.

[2] https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-b-key-concepts

5 PIA Methodology

The decision to conduct a PIA was taken quite late in the project's implementation. This means the output of the PIA could not have input into the system's design.

Fortunately, lengthy and considered consultations were held with key stakeholders during the design of the system, ameliorating that risk. These consultations are detailed in section 8.

Further, the privacy and access model is closely modelled on current work.

The PIA is being undertaken as a matter of good governance and future-proofing the project and helping inform learnings from the project.

The methodology has been viz:

1. Consult with LHD Privacy Manager and agree on need to assess for PIA.
2. Gain approval for PIA from Project Executive Sponsor.
3. Conduct Privacy Threshold Assessment.
4. Conduct PIA in accordance with OAIC and NSW Privacy Commissioner guidelines.[3]
5. Write PIA report, seek feedback/input and review.
6. Approve report and publish to project website.
7. Seek project board response to recommendations and publish response on website.

[3] https://www.oaic.gov.au/agencies-and-organisations/guides/pia-guide-qrt

6 PIA Governance

6.1 Roles and Responsibilities

The roles and responsibilities influencing the development of the privacy model and the compliance of the system with privacy legislation are listed below.

Table 1 PIA Roles and Responsibilities

Area of expertise	**Department**	**Resource**
Information and privacy protection	NNSW LHD, NSW MOH Legal	PM/Project Lead, LHD Privacy Manager
Information security	NNSW LHD and MOH PSA Team	PM/Project Lead, MOH Penetration Testing team
Technology and systems	NNSW LHD	PM/Project Lead
Risk management	NNSW LHD	PM/Project Lead
Law and ethics	NNSW LHD, NSW MOH Legal	Privacy Manager, Legal Officer
Compliance Analysis	NNSW LHD	PM/Project Lead

6.2 Terms of reference

The terms of reference of the PIA are limited to the steps generally recommended by the OAIC in order to conduct a PIA.

Thus, the PIA TOR are as follows:

1. Liaising with key stakeholders in preparatory work, report writing and follow up work.
2. Preparation of Privacy Threshold Assessment.
3. Identifying and consulting with stakeholders.
4. Mapping of personal information flows.
5. Privacy Impact Analysis and Compliance Check.
6. Privacy management—addressing risks.
7. Recommendations.
8. Preparation of report, approval chain and publishing to LHD’s Orion website.

6.3 Resources

Resources unofficially unassigned to the project thus far include:

- Tim Marsh, LHD Project Lead
- Di Goldie
- Joy Hathaway, LHD Privacy Manager

There is no budget as these staff members are currently either tasked with such assessments, or are funded via Integrated Care to assist.

The recommendations make clear that substantive work is required on privacy, with respect to consulting with patient representatives, strengthening privacy and legal documents and audit and review process.

The impact of these recommendations on resourcing and budgeting is discussed in the recommendations.

6.4 Timeframe

The PIA is to be completed before system go-live, nominally scheduled for early February 2017.

Since it requires extensive consultation and commenced late in the project, it may not be approved before this deadline.

Project go-live does not have a dependency on the PIA, but as a matter of good governance, and project authority, it would be ideal if it did.

7 Project Description

7.1 The problem

Currently, it’s extremely difficult for the care team of a chronic and complex care needs patient to effectively collaborate and manage the patient’s care. This is especially true for patients needing multi-disciplinary teams, requiring access to up-to-date key health information.

Due to information silos, not knowing who other team members are, lack of consistent information amongst other systemic issues, patients’ and clinicians’ experiences of care are poor. Patients don’t often receive truly integrated and seamless care.

Delivering quality, joined-up, care is truly difficult with poor patient experience and outcomes, systemic inefficiency and clinician job satisfaction all suffering.

7.2 The Solution

NNSW Integrated Care (NNIC) and its partners are implementing Orion Health’s Shared Care Tool across the Richmond and Tweed areas to a select list of General Practices in order to try and address these issues.

The Orion tool basically lets GPs put shared care plans in a central repository (cloud based) accessible by people the GP selects to involve in the care team, on an invitation/response basis (thereby satisfying Medicare requirements for 723 TCA item).

The tool is secured and also provides access to secure messaging, which is effectively email.

Members of the patient’s care team can see the care plan and add certain information to it so that the plan becomes an up-to-date living care plan, thus reducing the incidence of information silos.

7.3 Project Aims

The project aims are from the Project Initiation Document [2].

They include, but are not limited to, those discussed below.

The overarching aim for this project is to improve the care delivered to Chronic and Complex Care needs patients by multiple team members, improving their experience of health care. The project also aims to improve clinicians’ experience in delivering care.

The objectives in a business context are:

- To provide clinicians working with high-needs patients a system that supports:
  - new models of care with respect to team collaboration;
  - the ability to securely discuss patient care;
  - proactively manage tasks around patient care, and;
  - Tracking of progress against goals.

- Deliver Change Management (including communication, training and support framework) and clinical support to ensure the solution and the information it produces are integrated into new and existing work practices.
- Evaluating the POC against agreed criteria, provide an assessment to eHealth about use and efficacy of the system. This will provide NSW Health with useful insights into the system and its potential for state-wide adoption, including any augmentations required to address any shortcomings. The criteria require consultation with and agreement of relevant stakeholders (eHealth, Western NSW LHD and NNIC).

7.4 Strategic Fit

The concept of electronic shared care plans and secure message is aligned with Commonwealth Department of Health. In particular it aligns with the recommendations of the Primary Health Care Advisory Group's "Better Outcomes for people with Chronic and Complex Health Conditions".[4]

Moreover, the project strongly aligns with the direction the NSW Ministry of Health is taking in this area.

From an integrated care perspective, the concept fulfils the need to ensure a patient's care team has the same information and can communicate with each other electronically and securely.

To underline these points, the implementation of this system has been driven by user need, better patient care, and policy alignment.

7.5 Scope

7.5.1 Introduction

The project scope comprises several elements, viz:

- Time: the project will run for 12 months as a Proof of Concept ("POC") to prove the efficacy of electronic care plans. If the concept is deemed viable, a decision will be made before the expiry of 12 months on whether to continue with the Orion solution or pursue an alternative.
- Patients: patients will be adult patients (only) with chronic and complex care needs. Patients do not have access to the system at this stage.
- Geographic: the geographic footprint includes the Richmond and Tweed networks.
- Clinical users: clinical users include GPs, private service providers (allied health, specialists, pharmacy and others).
- Technical: the technical scope is discussed below.

7.5.2 Technical scope

The Technical scope comprises these elements:

[4] PHCAG report

- System Design: the system has been designed in close consultation with clinical users as well as resources with user experience/user interface design.
- GP Integration: the Orion system integrates with GP Practice Management Software ("PMS") Medical Director and Best Practice using a third-party, desktop-run "plugin" called EMR Connect (EMRC). There is a custom integration built for Genie users.
- Other integration: the system will also integrate with Medical Objects, a Secure Message Broker ("SMB").

7.6 Existing program links

The project is being implemented under the aegis of—and is therefore linked to—the North Coast's Integrated Care program.

More broadly, it's linked to the NSW Ministry of Health's Integrated Care program, and being implemented under its purview.

The project has loose links to other North Coast Integrated Care ("NCIC") projects and initiatives. The Orion Shared Care Tool can help strengthen, or work in concert with, the following initiatives and projects.

- Admission and Discharge Notifications for IC patients
- Integrated Care Collaboratives
- Health Literacy
- Patient Centred Care
- Patient Centred Medical Home
- Integrated Aboriginal Chronic Care
- End of Life Care

7.7 Project Owner

The project is co-owned by eHealth, the NNSW LHD and North Coast Primary Health Network (NCPHN).

From an implementation perspective, the NNSW LHD owns the implementation.

The project's governance closely aligns with project owners with implementation and project management layers as applicable.

The project is being co-funded by the NNSW LHD and NSW Health's eHealth department on the following basis:

- Services and build: eHealth
- Change management (training, workshops, installation): NNSW LHD
- Marketing/communications: PHN (video assets) and NNSW LHD (web assets)

7.8 Timeframe for decision-making

The timeframe for decision-making that affects the project's design has passed.

The design phase closed in May 2016.

Since PIA only came onto the radar in the latter half of the project, there is no scope to change the design of the system based on any privacy aspects. Changes would have to be canvassed as part of the post-trial environment. This would involve a decision to continue the platform, as well as making any improvements, as applicable.

7.9 Privacy elements

7.9.1 Information use and disclosure

As with all health information in NSW, the information in Orion is used and shared (disclosed) in accordance with the Health Records Information Privacy Act, Commonwealth Privacy Act and other relevant laws.

Users are required to acknowledge the terms of use at login to the system.

Patients are provided an information pamphlet indicating the basis of information collection, use and disclosure and on consenting to be enrolled to the system, accept the conditions governing collection of their information.

7.9.2 Security

Any user configured for access to the system can feasibly view the below information. The Privacy and Access model for the system that governs access is detailed in Table 15.

Where downloadable is indicated as “No” in Table 6, the information is generally able to be copy/pasted and/or printed which technically could constitute a download in very broad terms.

Although a patient cannot be removed entirely from the system as part of this POC, a system administrator can remove everyone from the patient’s circle of care, which means no one can access their record (this is reversible by the system administrator).

The password policy for the system is aligned to the NNSW LHD’s which is aligned the State-wide Standard governing passwords and information security.

Generally, this policy enforces strong passwords and regular password expiry.

The system maintains an audit view of system use, in the event a privacy breach occurred.

As is the case now, there is no reliable (with 100% confidence) method to prevent information being disclosed in breach of legislation. All users are bound to Federal and State legislation through system use (and accept the conditions at login) with LHD staff subject to disciplinary action in the event of breaches.

7.9.3 Quality

To maintain quality (accuracy), GPs are able to easily update the patient record, with the exceptions of medications.[5]

To a large extent, information entered in the system uses standard code sets, dropdown boxes and data/information libraries to standardise and ensure consistency of information.

GPs have noted that due to the nature of the system—improved visibility and sharing of care plans—care plan quality is likely to improve.

The project has implemented an evaluation measure around care plan quality to measure and interrogate that hypothesis.

However, there is some uncertainty around care plan quality, which explains the decision not to implement the Orion patient portal. Stakeholders indicated that as this was such a new way of working, they wanted to get "our own house in order first before opening the portal up to patients."

7.9.4 Information collected

The information collected (and its source) is in Table 6, in Section 10.4.

[5] Old medications cannot be removed. At the time of writing, this was the subject of negotiation/remedying between the project and Orion.

8 Stakeholders

Stakeholders consulted during the project are detailed below. Of key importance is the inclusion of a GP on the project board and in workshops who has a strong privacy background. This GP was able to focus the project on privacy aspects.

Table 2 Stakeholders

Stakeholder	Consulted stage	Methodology
GPs (5)	Design	Design workshops, design stage
LHD staff	Design	Design workshops, design stage
Patient-centred representatives	Design	Design workshops, design stage
Project Board	PIA output, recommendations	Report
Ministry of Health Legal Branch	PIA draft/release	Report
LHD Privacy Manager	PIA draft/release	Report
LHD Clinical Governance Unit	PIA draft/release	Report
LHD executive [TBC]	Final Report	Report
LHD CIO	PIA draft/release	Report
Consumer representatives	TBC – future	TBC

9 Information structure

9.1 Information Flows

A very high level picture of information flows between the various systems is depicted below.

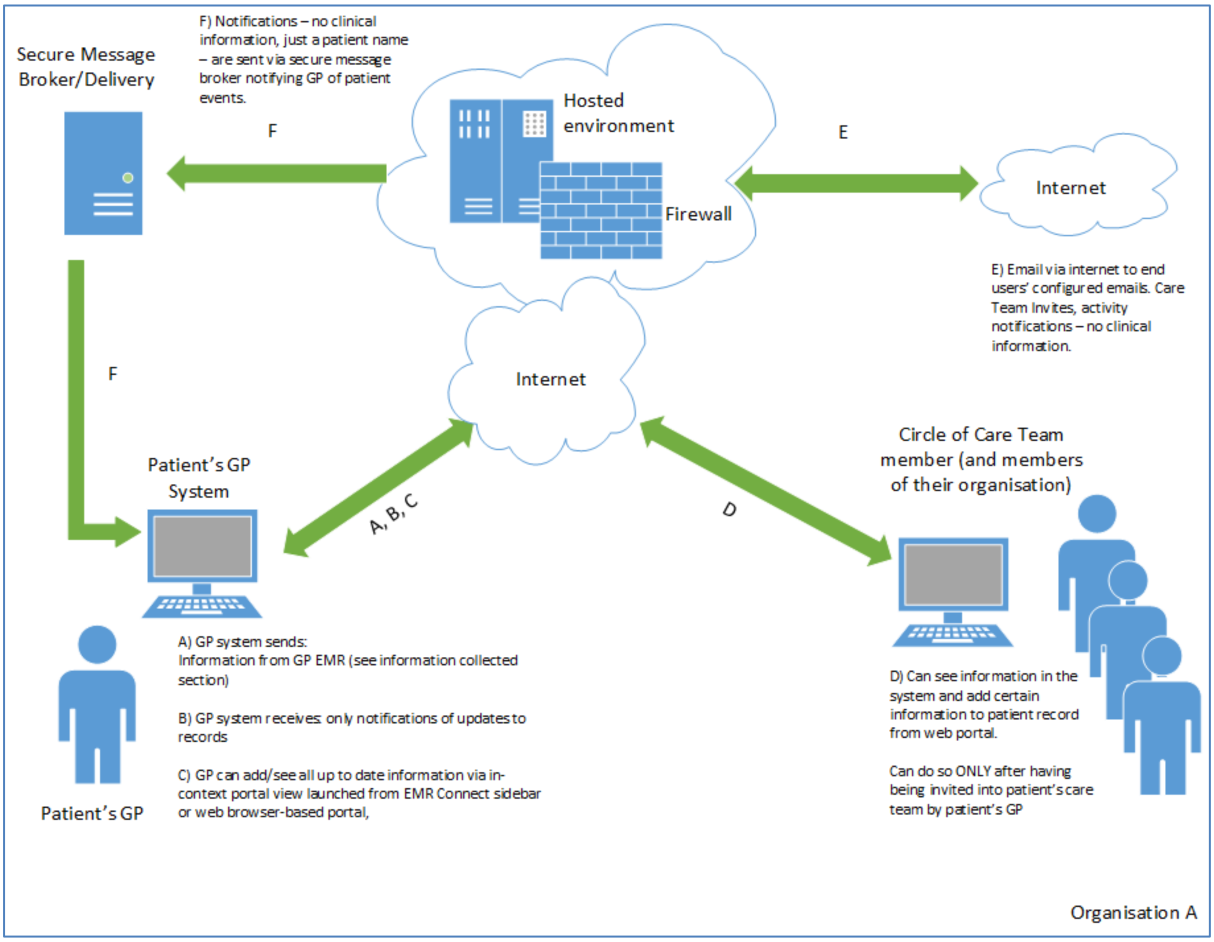
Note that this simplifies the information architecture but suitably captures the salient information and flows.

The steps for information collection are:

1. Patient is enrolled in the system. The GP's PMS is used as the source of truth, adding the patient to the system using: IHI, demographics (name, DOB, S, address) and allergies, medications and conditions from the GP system.
2. Patient demographics, conditions and allergies can be removed from the system. Medications at this stage cannot.
3. The GP can add any (or none) information from Table 6.
4. The GP can then invite clinicians into the care team.
5. Care team members can then also add any information noted as "Orion directly" in column A into the patient's record.
6. Certain documents are stored in the document tree, which can be printed to a printer or printed to a PDF file and in effect downloaded. These include:
    - Care plan (PHI included);
    - Care team invites/acceptance (no PHI);
    - Event note (could have PHI or clinical notes/information);
    - Legal documents (presence of and location, no PHI);
    - Assessments (type, outcome, context, could contain PHI);
    - Patient services (no PHI).
7. When certain events occur, notifications are sent to care team members. These notifications do not include clinical information or PHI.

Most notably:

- The enrolling GP's EMR is the source of truth for patient demographics, allergies, medications and conditions and this information is not alterable by anyone but the GP and GP system;
- No clinical information is sent in emails or notifications: only a patient name and a login to the portal.
- The hosted system will be penetration tested by the NSW Ministry of Health's Privacy, Security and Assurance team to ensure the system can withstand electronic attacks.



F) Notifications – no clinical information, just a patient name – are sent via secure message broker notifying GP of patient events.

E) Email via internet to end users' configured emails. Care Team Invites, activity notifications – no clinical information.

A) GP system sends: Information from GP EMR (see information collected section)

B) GP system receives only notifications of updates to records

C) GP can add/see all up to date information via in-context portal view launched from EMR Connect sidebar or web browser-based portal,

D) Can see information in the system and add certain information to patient record from web portal.

Can do so ONLY after having being invited into patient's care team by patient's GP

Figure 1 Information Flows

9.2 Access

9.2.1 Clinical and end users

The following entities will have access to the system and to PHI. Users will only be able to access the system after having been added by the project. Self-registration is not possible.

Users can only access a patient record when the GP adds them or someone from their organisation to the patient's care team.

Table 3 Access by users

Role	Access level	Comment
GP	Full	Enrolling GP
Practice Nurse	Full	Enrolling GP practice
Practice Manager	Read only	Enrolling GP practice

LHD	No edit/write access to actual snapshot care plans	Org based
Private providers	No edit/write access to actual snapshot care plans	Org base

More information on the access and privacy regime can be found in Appendix – Section 15.

9.2.2 Patients

Patients are not able to access the system directly.

Patient access is addressed in Sections 10.13 and 10.14.

9.3 Current information

The information to be solicited for inclusion in Orion currently exists in other, disparate electronic health records.

Orion is a mechanism for bringing together this information—breaking down the information silos—so that everyone in the patient's care team has the same up to date information.

9.4 Depth of information

The depth of information is limited to information deemed important in providing seamless integrated care for the patient.

Detailed clinical information will continue to be stored in hospital and GP EMRs and are not in scope for inclusion in Orion.

No new information is explicitly being collected or solicited, but it's possible that information like patient services is a new collection. That is, this type of information may exist in paper care plans used currently, but an audit of this is not in scope.

10 Privacy Analysis

10.1 Introduction

Where possible and applicable, the analysis is formed by assessing privacy impacts of the project against Australian Privacy Principles.[6]

However, it is important to note that the Health Privacy Principles established under the Health Records and Information Privacy Act 2002 (HRIP Act)[7] and the Privacy and Personal Information Protection Act 1998 (PPIP Act)[8] also apply. The principles in both of these Acts, to a large degree, comport with the principles set out in Commonwealth privacy legislation.

As Privacy is set by Legislation, the role is compliance. For the purpose of this document and consistency the Australian Privacy Principles were used.

Table 4 APPs and addressing in PIA

APP #	Addressed in PIA
APP 1 — Open and transparent management of personal information	Yes
APP 2 — Anonymity and pseudonymity	Yes
APP 3 — Collection of solicited personal information	Yes
APP 4 — Dealing with unsolicited personal information	Yes
APP 5 — Notification of the collection of personal information	Yes
APP 6 — Use or disclosure of personal information	Yes
APP 7 — Direct marketing	Yes
APP 8 — Cross-border disclosure of personal information	Yes
APP 9 — Adoption, use or disclosure of government related Identifiers	Yes
APP 10 — Quality of personal information	Yes
APP 11 — Security of personal information	Yes

[6] https://www.oaic.gov.au/agencies-and-organisations/guides/app-quick-reference-tool

[7] http://www.ipc.nsw.gov.au/hrip-act

[8] http://www.ipc.nsw.gov.au/ppip-act

APP 12 — Access to personal information	Yes
APP 13 — Correction of personal information	Yes

10.2 Open & transparent management (APP 1)

APP 1 states that:

"The APP entity must have ongoing practices and policies in place to ensure that they manage personal information in an open and transparent way. "

The APP provides further detail, contained in column 1 in Table 5 below.

Table 5 APP 1 analysis

APP	Response
Take reasonable steps to implement practices, procedures and systems that will ensure it complies with the APPs and any binding registered APP code, and is able to deal with related inquiries and complaints.	The project has designed the system, security, privacy, access and procedures with privacy at its core. Access is controlled and the privacy model and security regime are arguably stricter and more secure than current practices.
Have a clearly expressed and up-to-date APP Privacy Policy about how it manages personal information;	Use existing LHD/GP/other privacy complaint handling procedure, and addressed in the patient privacy and information pamphlet. Links to the patient's privacy policy will be clearly highlighted in the patient information and privacy pamphlet, provide to the patient on enrolment. Recommendation: address privacy breaches in training, and by adding information for system users to privacy page.
Take reasonable steps to make its APP Privacy Policy available free of charge and in an appropriate form (usually on its website)	Will have an APP-compliant Privacy Policy for a) website use (all users), b) system use (system users) and c) patient information. These policies will be reviewed, approved and made available on the project website. Recommendation: ensure privacy policies are APP compliant. Recommendation: add general web/app privacy policy for web/system use and patient privacy policy.

Upon request, take reasonable steps to provide a person or body with a copy of its APP Privacy Policy in the particular form requested.	Recommendation: make the privacy policies downloadable in PDF format on the website.

10.3 Anonymity (APP 2)

In accordance with APP 2, a patient wishing to be enrolled in the system but remain anonymous can do so by:

- Applying for a pseudonym IHI; and
- Create a linked non-identifiable MyHealthRecord; and
- Have that pseudonym identity used to create a patient record in the GP EMR; and
- Use that pseudonym record to enrol the patient in the shared care platform.

It's recommended that Legal confirm that IHIs are collected and used in accordance with the Healthcare Identifiers Act and Healthcare Identifiers Regulation 2010.

As of December 5th, 2016, Ministry of Health Legal advice confirms the project complies with the Act in the collection and use of IHIs.

10.4 Information collected (APP 3)

APP 3 details when an APP entity (the project) can collect solicited information and on what basis.

Information solicited and collected and how/if it is displayed is shown below.

Information collected is solicited from GPs, other members of a patient's care team, and the patient (or representatives) themselves.

Solicitation does not take the form of a direct request. Rather, there is an implied solicitation by system design: this system requires mandatorily or optionally some information in order to form an accurate patient record.

Table 6 APP 3 Information Collected

Information	Source	Displayed in system	Removable from system	Mandatory	Downloadable?	New collection?
Patient Name	GP system	Yes	No	Yes	No	No
Patient Address	GP system	Yes	No	Yes	No	No
Patient DOB	GP system	Yes	No	Yes	No	No
Patient Sex	GP system	Yes	No	Yes	No	No
Patient IHI	GP system	Yes	No	Yes	No	No
Patient Emergency Contact	GP system	Yes	Yes	Yes	No	No
Conditions	GP system	Yes	Yes	No	No	No
Allergies	GP system	Yes	Yes	No	No	No
Prescribed Medicines	GP system	Yes	No,	No	No	No

			discontinue meds in GP EMR			
Patient Carer/Family	Orion directly	Yes	Yes	Only Name, Relationship and Contact Phone # are mandatory	No	No
Patient Services	Orion directly	Yes	Yes	No	No	Possibly
Patient Legal Documents (document name and location, not actual document)	Orion directly	Yes		No	No	Possibly
Patient Assessments	Orion directly	Yes		No	No	Possibly
Next GP Appointment	Orion directly	Yes		No	No	
Patient Care Plan (Goals, Actions, Services, Assessments, Legal Documents, Care Team)	Orion directly	Yes	No	No	Yes (PDF)	No
Event Note	Orion directly	Yes	No	No	No	No

It is the view of the project that the project complies with APP substantively and in spirit and complies with the APP.

10.5 Unsolicited information (APP 4)

APP 4 deals with unsolicited information and the processes to be followed in the event unsolicited information is received.

In general, the Orion Shared Care Tool contains, and is intended to contain, solicited information only.

The only entry points for unsolicited information[9] are:

- User-facing helpdesk (hosted in the USA)
- Website contact forms (hosted in Australia)

To help manage the risk of unsolicited (PHI in particular), the project will:

1. Funnel all support requests primarily via the webpage (hosted in Australia). These forms will have PHI stripped out before being sent to the Helpdesk to manage ticketing.
2. Educate users not to enter PHI and unsolicited information into contact/helpdesk forms.
3. Use checkboxes (required) on forms on the website and helpdesk that the user will need to check to confirm they are not entering PHI.
4. Seek to have the Integrated Care website served entirely over SSL.

[9] https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-4-app-4-dealing-with-unsolicited-personal-information

At any stage, PHI will need to be deleted or stripped out. For example, if a user added PHI to a website submission form, the submission can be manually forwarded to the helpdesk after having PHI stripped out. The form entry can then be deleted from the database thus satisfying the unsolicited information destruction requirements of APP 4, unless

10.6 Notification of collection (APP 5)

APP 5 "Outlines when and in what circumstances an APP entity that collects personal information must notify an individual of certain matters."

At its core, this APP is about ensuring that the project notifies patients and end users of information collected and how it is used.

Broadly, "*these matters include:*

- *the APP entity's identity and contact details*
- *the fact and circumstances of collection*
- *whether the collection is required or authorised by law*
- *the purposes of collection*
- *the consequences if personal information is not collected*
- *the entity's usual disclosures of personal information of the kind collected by the entity*
- *information about the entity's APP Privacy Policy*
- *whether the entity is likely to disclose personal information to overseas recipients, and if practicable, the countries where they are located.*

"An APP entity must take reasonable steps, before, or at the time it collects personal information. If this is not practicable, reasonable steps must be taken as soon as practicable after collection."

The project satisfies this requirement by providing patients with an information and privacy pamphlet before acquiring consent. The pamphlet addresses these matters.

10.7 Information use and disclosure (APP 6)

10.7.1 Use

On use, APP 6 lists the below items for consideration. Following each is a statement highlighting how the project complies.

1. All the planned uses of the personal information, including infrequent uses.

The personal information will be used for the purposes of identifying patients in the shared care system, and putting key information that can improve their care, in one spot. The information is used to provide better-connected, more integrated care.

2. How all these uses relate to the purpose of collection.

Without collection, the intended use cannot occur.

3. Measures in place to prevent uses for secondary purposes or to ensure that any secondary uses are permitted under the APPs.

Users cannot use the information for a secondary purpose and are bound by relevant Privacy Act and NSW HRIP Act obligations. LHD staff are also bound by the NSW Ministry of Health Code of Conduct[10].

Allowed secondary uses are permitted and limited to benchmarking, evaluation and internal business use.

4. If information may be used for a secondary purpose, identify and describe:
    - Whether consent is required for the secondary use
    - if the use is related or directly related to the purpose of collection
    - Whether an individual can refuse consent for secondary uses and still be involved in the project.

The secondary uses meet the "reasonably expect" tests of APP 6.2 and is disclosed to the patient in the Patient Information and Privacy Pamphlet and in the Privacy Policy, to which the patient consents to before enrolment.

Use is directly related to the purpose of collection.

Secondary use is for anonymised internal reporting, evaluation and benchmarking (counting number of patients, by practice, GP and length of enrolment) and not for data/record linkage and marking. The secondary use is viewed as being non-impactful to privacy but important to the proper operation of reporting and evaluation regime. Therefore if a patient refuses to provide consent secondary use, their records would have to be excluded from reporting/evaluation use. This would necessitate a register of secondary-consent-declined patients, and exclusion of these records from any reporting/benchmarking.

It's recommended that such a register not be implemented as a) it is in and of itself a risk, b) is a non-trivial amount of work to implement and c) the privacy risk from secondary use is minimal and proportional to use.

5. Any consequences for individuals who refuse consent.

Individuals who do not consent to enrolment, and subsequently refuse collection and use, cannot be enrolled on the system. It is difficult to say if this will impact on their care as it is unclear how impactful Orion will be on patient experience and outcome. However, there would not be any change to or impact on the way care continues to be delivered to the patient.

6. How individuals will be involved in decisions if new, unplanned purposes for handling personal information occur during the project.

Typically, changes to collection, use and privacy more generally are made with 3 months warning.

Patients would be provided an updated information and privacy pamphlet at the earliest opportunity.

The system requires that GP indicate maintenance of consent when a care plan review is undertaken. This typically occurs at 6 month intervals but can occur as often as every 3 months or at 12 month

[10] http://www0.health.nsw.gov.au/policies/pd/2015/PD2015_035.html

intervals. This means that at worst, a patient could not be re-consented and made aware of changes to information use 9 months after a change (12 month interval less 3 month notification period).

It is recommended patient representatives be consulted on whether this an acceptable gap in notification.

7. Data linkage or matching, which involves aggregating or bringing together personal information that has been collected for different purposes, has additional privacy risks. If your project will involve data linkage or matching, identify and describe:
    - any intention or potential for personal information to be data-matched, linked or cross-referenced to other information held in different databases (by you or other entities)
    - how data-matching, linking or cross-referencing might be done
    - any decisions affecting the individual that might be made on the basis of data-matching, linking or cross-referencing
    - safeguards that will be in place to limit inappropriate access, use and disclosure of the information
    - audit trails and other oversight mechanisms that will be in place
    - protections in place to ensure data linkage accuracy and that individuals will not be adversely affected by incorrect data matching.

Does not apply: patient records will not be linked to other data sets.

10.7.2 Disclosure

On APP 6-disclosure, it is recommended that the project "*identify and describe:*

- *to whom, how and why the personal information will be disclosed*
- *whether the disclosed information will have the same privacy protections after it is disclosed*
- *whether the information is to be published, or disclosed to a register, including a public register*
- *whether an individual will be told about the disclosure and what choices they have (such as publishing or suppressing their information)*
- *whether the disclosure is authorised or required by law, and if so, which law*
- *whether the personal information will be disclosed to overseas recipients."*

These points are addressed in Table 7 below.

Table 7 APP 6 Disclosure analysis

APP question	Reponse
To whom, how and why the personal information will be disclosed	Information is disclosed between members of a patient's care team and possibly family members. IN the event of an emergency, it may be disclosed to other parties in

	accordance with relevant legislation.
Whether the disclosed information will have the same privacy protections after it is disclosed.	Yes.
Whether the information is to be published, or disclosed to a register, including a public register	No.
Whether an individual will be told about the disclosure and what choices they have (such as publishing or suppressing their information)	Patients will be told about the disclosure and will have the option of participating via an anonymous IHI and anonymous MHR.
Whether the disclosure is authorised or required by law, and if so, which law	Disclosure is authorised by the Privacy Act 1998, 16B (1) (a) and (b) Permitted health situations, and under the reasonable expectations test in APP 6.2 (a) (i) and inline with the principles contained in APP 6.1, 6.2, 6.3 and 6.4.
Whether the personal information will be disclosed to overseas recipients.	Does not apply. Risk here is disclosed and detailed in Section 10.9.

The project complies on Disclosure by a) having addressing these points and b) outlining disclosure in the patient information pamphlet.

10.8 Direct Marketing (APP 7)

Patient information is not collected for the purposes of direct marketing.

End user (clinician) emails can be used for business purposes, such as notifying of system outages, but are not used for direct marketing.

10.9 Cross border disclosure (APP 8)

Reasonable steps have been taken to ameliorate the risk and occurrence of cross border disclosure of information either from the system or contact forms.

At its core, the system is designed to be used by NSW and QLD clinicians, with the system hosted in NSW.

These steps include:

1. Turning off a feedback “widget” that comes with the Orion platform. This widget submits to an overseas location, where the PHI is stripped out. It was switched off for this reason.
2. Ensuring the system does not have elements hosted in, or submitting to/via, overseas locations.

Moreover, as detailed in 10.5, the helpdesk is hosted in the USA, thereby introducing a low risk that PHI could be sent to the helpdesk via the helpdesk email.

To mitigate this risk, we will:

3. Funnel all support requests primarily via the webpage (hosted in Australia). These forms can have PHI stripped out before being sent to the Helpdesk to manage ticketing. This will be done manually to begin with so we can observe how much PHI is actually put in forms.
4. Educate users not to enter PHI into contact/helpdesk forms or email to the helpdesk. Where users send PHI to the helpdesk, the ticket will be altered and PHI stripped out as soon as possible.
5. Use checkboxes (required) on forms on the website and helpdesk that the user will need to check to confirm they are not entering PHI.

10.10 Government Identifiers (APP 9)

Strict rules govern the collection and use of government identifiers.[11]

APP 9 states *"Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual."*

Orion uses the Australian Government's Individual Healthcare Identifier (IHI), sourced from GP systems. However, Orion does not use this identifier for the purposes of matching the patient with external systems.

The GP system obtains and matches the patient's IHI in that system and simply provides the IHI to Orion as a unique identifier.

The Orion Shared Care tool doesn't disclose the IHI to any other systems.

The IHI appears in 3 key contexts in the platform:

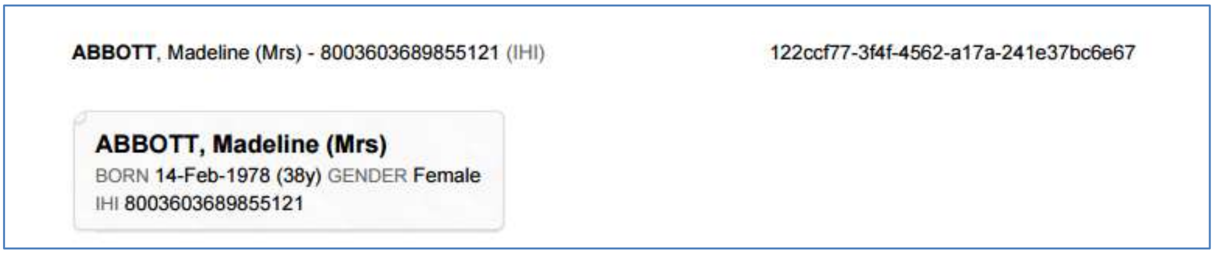
- Patient record
- Patient lists
- Patient care plan

Examples are shown below of test patients and IHIs (not real patients or IHIs).

Recommendation: that legal advice is being sought from the Ministry of Health whether the IHIs need suppression from display.

As of December 5th, 2016, Ministry of Health Legal advice confirms the project complies with the Act in the collection and use of IHIs.

[11] https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-9-app-9-adoption-use-or-disclosure-of-government-related-identifiers

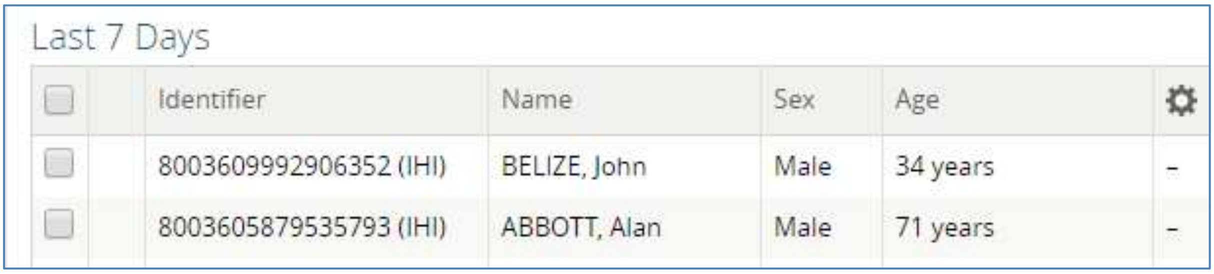


ABBOTT, Madeline (Mrs) - 8003603689855121 (IHI)

122ccf77-3f4f-4562-a17a-241e37bc6e67

ABBOTT, Madeline (Mrs)
BORN 14-Feb-1978 (38y) GENDER Female
IHI 8003603689855121

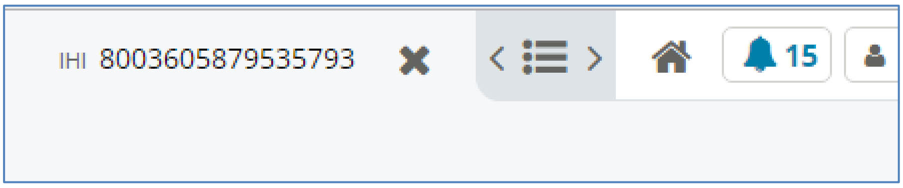
Figure 2 Care Plan header



Last 7 Days

□	Identifier	Name	Sex	Age	⚙
□	8003609992906352 (IHI)	BELIZE, John	Male	34 years	-
□	8003605879535793 (IHI)	ABBOTT, Alan	Male	71 years	-

Figure 3 Patient list



IHI 8003605879535793 ✖

Figure 4 Patient banner in portal

10.11 Quality (APP 10)

APP 10 states that *"An APP entity must take reasonable steps to ensure that the personal information it collects is accurate, up-to-date and complete.*

"An APP entity must take reasonable steps to ensure that the personal information it uses and discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant."

The idea with an electronic shared care plan, hosted centrally in the cloud, is that care team members will help ensure information currency and quality by helping "curate" the information by updating it on a constant and consistent basis.

It is acknowledged that a) team members having access to the same information and b) information that is accurate is a key part of quality patient care.

Users of the Orion system are committed to this ideal.

GPs play a key part in maintaining quality by acting as the custodian/lead for the patient information and by ensuring their GP systems update the patient record regularly (per appointment). This responsibility can be communicated and reinforced during training.

A way to help measure this is to take a select number of patient records after a period of operation and interrogate them for quality, accuracy and currency. The parameters by which accuracy, quality and currency are to be defined but as an example, a comparison between the records in Orion and the GP EMR could be made for these datasets:

- Allergies
- Medications
- Conditions
- Demographic (updated automatically from Orion, so should be a non-issue)
- Patient services
- Assessments
- Legal documents
- Validity of care plan

The below recommendations are made:

- That a select number of records be collected after a period of operation, and at planned intervals, and be analysed for quality.
- GP and end user training cover off information quality obligations, particularly for GPs.

10.12 Information storage & security (APP 11)

APP 11 states that *"An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances."*

10.12.1 Storage and security

Identify and describe:

1. Security measures that will protect the personal information from loss, unauthorised access, use, modification, disclosure or other misuse (including for contracted service providers).
2. How information will be transferred between sites.
3. How personal information will be protected if it will be managed by someone else.
4. Who will have access.
5. Who will authorise access.
6. The systems that will prevent and detect misuse or inappropriate access.
7. What action will be taken if there is a data breach.[10]
8. Will control procedures be in place requiring authorisation before personal information is added, changed or deleted?
9. Is staff training adequate to fulfil the reasonable steps required?

Table 8 Storage and security analysis

APP	Response
Security measures that will protect the personal information from loss, unauthorised access, use,	Strong passwords with expiry and policy aligned with LHD/NSW Health password policy (regular

modification, disclosure or other misuse (including for contracted service providers).	expiry etc). Individual logins. Users subjected to Privacy Act, HRIP Act and PPIP Act. LHD staff subject to code of conduct and disciplinary action.
How information will be transferred between sites.	Electronically and securely via a single hosted cloud based portal. Physical transfer does not occur.
How personal information will be protected if it will be managed by someone else.	Does not apply.
Who will have access?	Only authorised personnel.
Who will authorise access?	The project team, based on verified requests for access.
The systems that will prevent and detect misuse or inappropriate access.	The system provides for a Privacy Officer role that can monitor system use, searchable by patient if needed. In the event of a privacy complaint or breach, any reporting requirement can be fulfilled. [Recommendation: annual audits be conducted, approved by management and funded, or else conducted by existing audit resources.
What action will be taken if there is a data breach.	Formal investigation (using existing LHD framework) would be launched for any alleged breach of privacy. LHD staff breaching privacy can be subject to disciplinary action and/or termination. Existing policies to manager all users are Commonwealth and State Policy Legislation Action: seek advice on current IT system data breach processes.
Will control procedures be in place requiring authorisation before personal information is added, changed or deleted?	No. Information comes from GP systems or other clinicians, who are already bound by Codes of Conduct and information quality clauses of the Privacy Act.
Is staff training adequate to fulfil the reasonable steps required?	Yes.

10.12.2 Retention and destruction

Identify and describe:

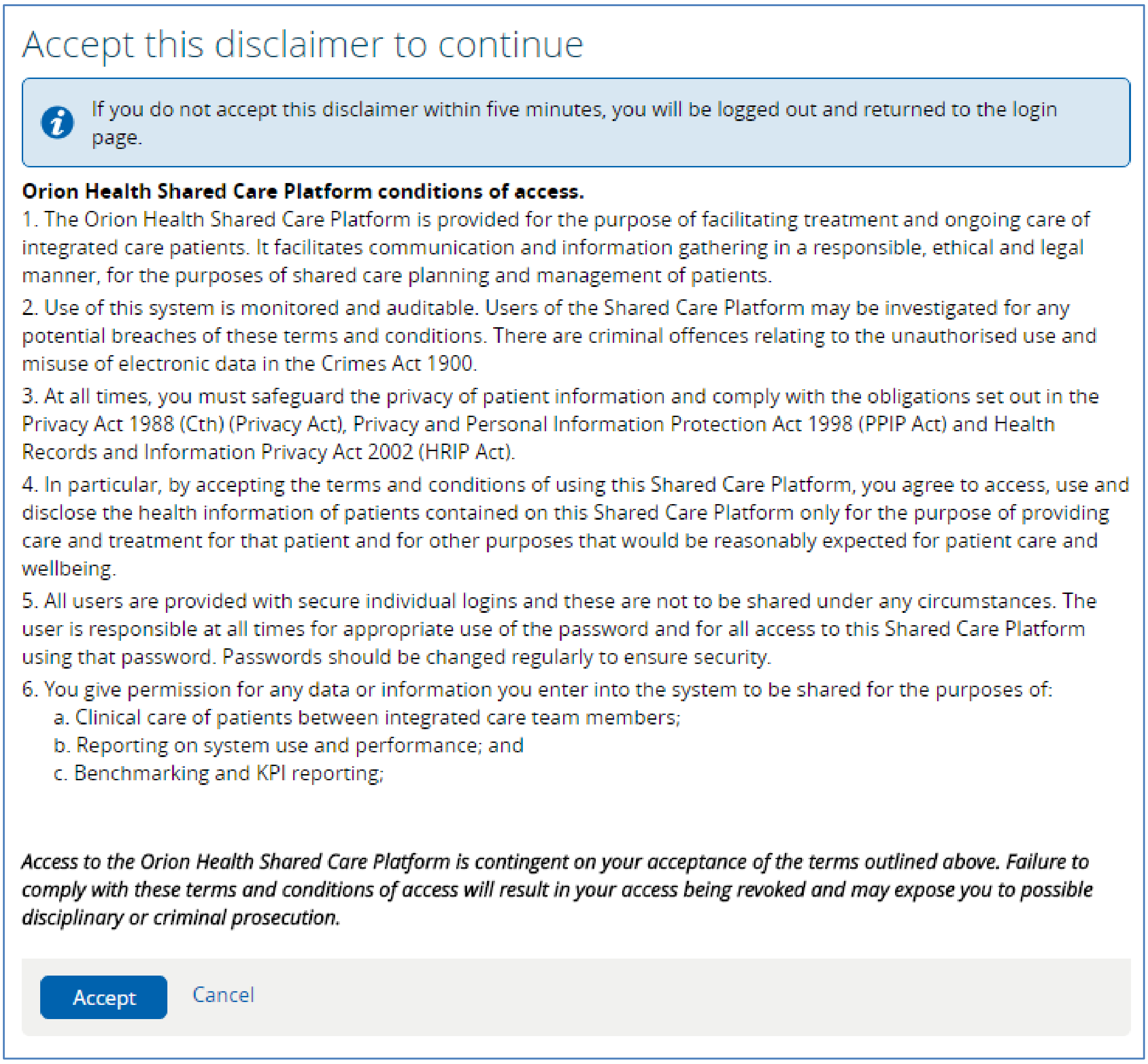
- When personal information will be de-identified or destroyed;
- How this will be done securely;
- Whether an information retention policy and destruction schedule is in place; and
- How compliance with this policy and any relevant legislation about record destruction will be assessed.

Table 9 Retention and destruction analysis

APP	Response
When personal information will be de-identified or destroyed	Section 10.4 and 10.9 outlines how communications will be de-identified or destroyed. Personal information is de-identified for the purposes of reporting and evaluation (i.e. a count of the number of patients in the system). Personal information is not destroyed as a matter of practice. A patient’s record is maintained in the system (on death, de-enrolment, other) but access to it by anyone can be prevented except in the event of a legal or other lawful requirement. A patient’s record cannot be expunged from the system by an operator or database operation.
How this will be done securely	De-identification is completed by LHD personnel, so will be done securely and in accordance with relevant legislation. Information is stored electronically so can be destroyed.
Whether an information retention policy and destruction schedule is in place	Orion data retention will follow Corporate Records Act – data cannot be destroyed until 7 years after death, or last admission, before archiving occurs.
How compliance with this policy and any relevant legislation about record destruction will be assessed.	Agreed review period for PIA and related policies and processes. Recommendation added.

10.12.3 Steps to manage

Upon logging in to the system, users must accept conditions of use, which are displayed in Figure 5.



Accept this disclaimer to continue

If you do not accept this disclaimer within five minutes, you will be logged out and returned to the login page.

Orion Health Shared Care Platform conditions of access.

1. The Orion Health Shared Care Platform is provided for the purpose of facilitating treatment and ongoing care of integrated care patients. It facilitates communication and information gathering in a responsible, ethical and legal manner, for the purposes of shared care planning and management of patients.
2. Use of this system is monitored and auditable. Users of the Shared Care Platform may be investigated for any potential breaches of these terms and conditions. There are criminal offences relating to the unauthorised use and misuse of electronic data in the Crimes Act 1900.
3. At all times, you must safeguard the privacy of patient information and comply with the obligations set out in the Privacy Act 1988 (Cth) (Privacy Act), Privacy and Personal Information Protection Act 1998 (PPIP Act) and Health Records and Information Privacy Act 2002 (HRIP Act).
4. In particular, by accepting the terms and conditions of using this Shared Care Platform, you agree to access, use and disclose the health information of patients contained on this Shared Care Platform only for the purpose of providing care and treatment for that patient and for other purposes that would be reasonably expected for patient care and wellbeing.
5. All users are provided with secure individual logins and these are not to be shared under any circumstances. The user is responsible at all times for appropriate use of the password and for all access to this Shared Care Platform using that password. Passwords should be changed regularly to ensure security.
6. You give permission for any data or information you enter into the system to be shared for the purposes of:
   a. Clinical care of patients between integrated care team members;
   b. Reporting on system use and performance; and
   c. Benchmarking and KPI reporting;

Access to the Orion Health Shared Care Platform is contingent on your acceptance of the terms outlined above. Failure to comply with these terms and conditions of access will result in your access being revoked and may expose you to possible disciplinary or criminal prosecution.

Figure 5 Terms of use splash screen

10.13 Access to personal information (APP 12)

Broadly, this APP describes:

- How individuals can access their personal information, including any costs to the individual.
- How decisions will be made about requests from individuals for access to or correction of their information.

The Orion system will comply with this APP by:

1. For requests via the LHD, being made subject to existing access to personal information process; and
2. For requests via Private Service Providers including GPs, maintaining a process for those providers; and by

3. Allowing patients to view their record when in an appointment with anyone in their care team.

There may need to be a process (form) for users and patients to submit access requests. Advice needs to be sought on how to approach this: do current policies apply (for example, do patients pay for access etc).

Patients are not able to be given logins to the system at this stage, but patient access by the Orion patient portal has been canvassed for implementation after the 12 month trial.

For access requests where a copy of information is requested, the Project is able to print copies of all information pertaining to that patient and provide in PDF format. It is recommended that this information be provided to the patient using existing processes.

10.14 Corrections to information (APP 13)

APP 13 outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals.

At a practical, APP asks a set of questions, which are responded to in Table 10 below.

Advice needs to be sought on whether it is appropriate for patients to pay for corrections.

Table 10 Corrections to information

APP Question	Response
Will individuals be made aware of how to request correction of their personal information?	Yes – add link to privacy page on website, linked to a correction request form
Will reasonable steps be taken to correct information that is not accurate, out of date, incomplete, irrelevant or misleading, having regard to the purpose for which the information is held?	Yes
Are processes in place for responding to requests from individuals to correct personal information?	There will be – to be confirmed, how to capture and direct requests. Records? Orion team. Lead GP?
Are processes in place for identifying and correcting personal information that is inaccurate, out of date, incomplete, irrelevant or misleading?	Yes - same process as applies to EMRs now. Clinicians can correct certain information. Changes to certain fields are not possible in Orion.
Will individuals be informed about the reasons if	Yes

a request for correction is denied?	
Are processes in place for associating a statement with personal information if a request for correction is denied?	Yes – implement a corrections process including the fields that can be corrected, or have a statement associated (event note a possible avenue).

10.15 Compliance Summary

A summary of APP compliance is shown in Table 11 below. Recommendations are made where required.

Note that a recommendation may be as simple as a follow up task (add a link to a website/brochure) or as complex as calling for development of a policy or process.

A judgement of compliance is made on the author's best interpretation of privacy legislation and the APPs.

It is recommended that the Project Board seek independent or expert review to ensure compliance analysis is correct.

Table 11 APP compliance summary

APP	Compliance	Comments
1 - Transparency	Will comply	4 recommendations made.
2 – Anonymity	Complies	1 recommendation made.
3 – Solicited	Complies	
4 – Unsolicited	Complies	1 recommendation made.
5 – Notification	Complies	1 recommendation made.
6 – Use and disclosure	Complies	2 recommendations made.
7 – Direct marketing	Complies	
8 – Cross border disclosure	Complies	
9 – Government identifiers	Complies	1 recommendation made.
10 – Quality	Complies	1 recommendation made.
11 – Security	Will comply	5 recommendations made.

12 – Access	Will comply	1 recommendation made.
13 - Corrections	Will comply	3 recommendations made.

11 Privacy Analysis Summary

11.1 Overall privacy statement

Overall, the privacy impact of this project is viewed as low. Whilst some new information may be solicited, it is collected in the interests of providing better health care to the patient. Much of the information that will be housed in the system already exists in other electronic databases, be it GP EHRs, hospital EMRs, federal registers or private provider clinical notes.

The project is assessed as having acceptable privacy outcomes, and unacceptable privacy impacts.

11.2 Impact Assessment

In assessing the privacy impacts and therefore risks, the APP framework suggests some key questions to help frame any impacts. These are included in Table 12 below.

Table 12 Privacy Impact Assessment

Impact question	Response
Do individuals have to give up control of their personal information?	No, individuals will not give up control of their personal information.
Will the project change the way individuals interact with the entity, such as through more frequent identity checks, costs, or impacts on individuals or groups who do not have identity documents?	No change.
Will decisions that have consequences for individuals be made as a result of the way personal information is handled in the project (such as decisions about services or benefits)?	No detrimental effect.
Is there a complaint-handling mechanism? If yes, is it visible, comprehensive and effective?	Existing complaint frameworks. Education needed during training and via a complaint policy fact sheet.
How will you handle any privacy breaches?	Use existing complaint/privacy frameworks. Users subject to terms of use, NSW MoH Code of Conduct, and applicable privacy legislation.
Are there audit and oversight mechanisms in place (including emergency procedures) in case the system fails?	Annual audit capability, recommendation made as part of PIA for regular audits.
Does the project recognise the risk of function	Yes, risk recognised. Linkage may occur in the

creep? (For example, is there an interest in using the personal information collected for the project for other purposes that might occur in the future?)	future but would have to go through governance and notification to patients.
How valuable would the information be to unauthorised users? (For example, is it information that others would pay money for or try to access via hacking?)	Less valuable than other health information as it is high level meta-type information. Identifiers available in the system are name, address, DOB, sex and IHI. Medicare number is suppressed. Identity theft risk depends on a lot of variables such as expertise and skill of thief, as well as susceptibility of target system/entity. Printed on a care plan is a patient's name, DOB, sex and IHI. Address is not displayed. Unable to say if others would pay for it.
How consistent is the project with community values about privacy? (You are likely to need to undertake some form of consultation in order to assess this, but could also look at community responses to similar projects, or research into community attitudes about privacy).[11]	Very consistent, relative to the benefits derived. No more privacy impact than current health information collection.

11.3 Detailed assessment

Question: to what extent is the data collected a necessity?

The information collected is viewed as being a minimum necessary collection of information that allows clinicians to hold an informed and complete view of the patient and their circumstances. This view allows clinicians to better-deliver care in a more integrated manner that seeks to provide a better experience to the patient.

Extraneous information is not solicited and information seeks to meet ALCOA, by being Attributable, Legible, Contemporaneous and Accurate. The tool is not able to meet the Originality standard as the original notes are stored in GP, LHD and other EMRs.

Question: what are the risks of privacy impacts on individuals (both serious and more minor) as a result of how personal information is handled?

A privacy impact is subjective, depending on the prevailing views of the individual.

Currently, the type of information that will be held in this system is already stored electronically in GP, hospital or other EMRs, or on paper. The information is thus already at risk of mishandling or malfeasance.

Arguably, centralisation of information presents some increased privacy risk due to the nature of consolidation.

However, privacy risk is balanced with the expected benefits to patient care and experience by creating a more seamless, integrated care experience. This is the "proportionality" test of the APP.

This hypothesis can be tested during the evaluation using qualitative surveys and counts of privacy incidents or issues (if any)

Question: are the privacy impacts necessary or avoidable?

Privacy risks, and potential impacts, are viewed as necessary in the context of improved patient care and experience.

Each risk has some mitigation policy (refer Table 13) either through law or binding obligations, or system design, that aims to manage the risk.

Question: are there are any existing factors that have the capacity to mitigate any negative privacy impacts?

In addition to privacy-focussed system design, governmental and organisational policies, laws and requirements are already in place to help manage privacy risk.

Question: how do the privacy impacts affect the project's broad goals?

The potential privacy impacts do not impact on the project's goals as the risks are managed and potential impacts proportional to risks and benefits.

Question: does the project affect an individual's choices about who has access to their personal information?

There is no effect on individuals' choices. It is expected that a GP would discuss involvement of other practitioners in the patient's care, as is the case (or should be the case) now for Team Care Arrangements. Thus, since the project doesn't seek to change the GP's processes with team-based arrangements it may the case that the GP does, or does not, discuss who will be involved in the patient's care team.

Arguably, the Orion system strengthens a patient's control over who can see their information by requiring someone (or someone in their organisation) to be invited into the care team before being able to see the record.

Access can be extended to other providers at a patient's request.

A patient is able to withdraw consent at any point, and all team members will be removed, meaning no one can access the patient record (except in the case of system breach or for audit/subpoena reasons by a system administrator).

Question: how does the use of personal information in the project align with community expectations?

As no community (patient/consumer) consultations have occurred yet, it is difficult to answer this with any authority.

However, based on previous feedback on how patients expect, and would like, their care and care services to be "joined up", and given how information is currently collected, stored and shared, it is the project's analysis that the project aligns with community expectations.

11.4 Privacy Risks and Mitigation

Broadly, the project has aimed to ameliorate privacy risk by:

- Implementing privacy protections through governmental and organisational legislation, policies and procedures.
- Enhancing privacy by technical design: modelled on access to current systems, strengthened through an invite-to-record model.
- Using privacy-enhancing technologies, such as secure electronic communication, to try and reduce the reliance on fax and paper delivery, or non-secure email (e.g. Gmail to Hotmail).
- Using education strategies to reinforce privacy protection obligations and risks in the platform.
- Collecting the bare minimum information to make the system useful.
- Placing transparency and accountability at the core of the approach of the project to privacy: place all privacy policies and the PIA on the website, and by using best practice templates (e.g. APP-compliant privacy policy).
- Parsing all patient collateral (e.g. information brochures) through a Health Literacy Officer to ensure the privacy protections information is easy to understand and written in plain English, to a Grade 11 (maximum, preferably Grade 8) level.

Privacy risks have been identified, along with a risk of each. These are listed in Table 13 below.

Table 13 Privacy Risk and mitigation

Risk	Likelihood	Mitigation	Impact
Password shared (security risk)	Possible	Education, reinforce LHD staff obligations to Code of Conduct and all users' obligations to Privacy Act. To reduce risk, ORG-based access to record designed to improve continuity of care.	Low, impacts audit integrity, also a security risk.
Password security (poor)	Possible	Password policy aligned with NSW Health SWIS policy.	Low, strong passwords enforced.
Computer left with browser open (security risk)	Possible	Inactivity logout of 1 hour for web portal, 2 hours for GP EMRC widget (location based security as added layer).	Low.
Printing to paper (information currency and contemporaneousness risk)	Likely	Reinforce printing to paper for intended use only and staff's obligation to help maintain information security.	Low, patient identifiers minimised on printed material.

Printing to PDF (information currency and contemporaneousness risk)	Likely	Supported behaviour for Care Plans, for handing to patients or storage in another EMR. Reinforce use of printing for intended purpose only.	Ibid.
Unlawful use/disclosure	Possible	This is not a new risk, and is currently managed in existing frameworks including codes of conduct and obligations under	Low.
IT system at GP (security risk)	Possible	In general, GP practices must have strict IT standards in order to meet RACGP accreditation. Whilst these standards do govern security, the project has implemented a range of security and privacy protection measures “just in case”.	Low.
IT system at PSP (security risk)	Possible	There is not a single minimum IT and information management standard for practitioners working in healthcare. However, it is assumed that most practices try and meet some level of information management and security standard. As a risk management “just in case” measure, an MOU could be formed for each practice to sign stating compliance with the Privacy Act and APPs.	Low (mitigated with other measures).
System breach – cyber attack	Possible	Pen testing by eHealth to expose vulnerabilities, and housing in LHD IT infrastructure.	Low-medium.

11.5 Recommended strategies

See Section12 - Recommendations for recommended strategies. These recommendations address privacy risks either directly or systemically.

Broadly, the recommendations cover:

1. Seeking consumer feedback on privacy issues and impacts.
2. Seeking legal advice on applicable recommendations.
3. Subjecting the PIA, PIA response and PIA review to independent review.
4. Actioning non-contentious items (i.e. creating a web form, or adding links) ASAP.

12 Recommendations

A table of recommendations is contained below. A PIA response should be completed by the business, identifying which recommendations it accepts. The project should then be resourced to implement the accepted recommendations.

Table 14 Recommendations summary

APP	Rec #	Recommendation
1	1	Address privacy breaches in training, and by adding information for system users to privacy page.
1	2	Add general web/app privacy policy for web/system use and APP-compliant patient privacy policy.
1	3	Make sure links to privacy policy are in brochures.
1	4	Recommendation: make the privacy policies downloadable in PDF format on the website.
1	5	Seek advice on privacy breach handling procedure: should the system be subjected to existing frameworks, or have a new process.
1	6	Engage consumer representatives in any further privacy changes, using existing processes and forums.
2	7	Seek clarification on whether IHIs are collected and used in accordance the Healthcare Identifiers Act and Healthcare Identifiers Regulation 2010. *Note: MoH Legal confirmed via email advice on 5/12/16 that collection and use of IHIs in Orion are consistent with legislation.*
4	8	As much as possible, funnel all support requests primarily via the webpage (hosted in Australia). These forms can have PHI stripped out before being sent to the Helpdesk to manage ticketing.
4	9	Educate users not to enter PHI (Personal Health Information) and unsolicited information into contact/helpdesk forms.
4	10	Use checkboxes (required) on forms on the website and helpdesk that the user will need to check to confirm they are not entering PHI.
4	11	Seek to have the Integrated Care website served entirely over SSL.
5	12	Seek review of the Patient Information and Privacy Pamphlet.
6	13	[Use] That secondary use cannot be declined as it would result in creation of a declined-secondary-use register (with IHI), which a) it is in and of itself a risk, b) is a non-trivial amount of work to implement and c) the privacy risk from secondary use is minimal and proportional to use.

6	14	Seek advice on whether the notification period for changed privacy policy (potentially 9 months or more), is too long. If so, seek advice on how to notify patients of policy change.
9	15	Seek legal advice on whether IHI suppression is needed from the system. IHIs are used to uniquely identify patients. (Update 5/12/16: MOH legal advice implies this is not needed).
10	16	That a select number of records be collected after a period of operation, and at planned intervals, and be analysed for quality.
10	17	That GP and end user training cover off information quality obligations, particularly for GPs.
11	18	Recommended that an annual audit function (at a minimum) and resource be approved. Health policy states: System/Application administrator should monitor the event logs created by the system/application to ensure that inappropriate behaviour or potential intrusions are recognised and addressed. Audit log should be examined at a minimum every fourteen (14) days. The responsibilities should be formally assigned and documented in operational management procedure. HS/ 2013_14§3 Given that this project is a Proof of Concept, it's proposed that this be adopted if the project is scaled beyond the 12 months. Moreover, it's proposed that this be facilitated under existing procedures, frameworks and resourcing.
11	19	Seek advice on current IT system data breach processes.
11	20	That a record delete (expunge) function be requested of Orion post 12 months, in accordance with below recommendation.
11	21	Seek advice on whether a patient request for removal of their record from the system comports with Corporate Records Act requirements for retention.
11	22	Redacted – retention in accordance with Corporate Records Act. ~~Seek advice on whether an information retention and destruction policy needs implementation or if existing policies can be applied.~~
11	23	That a review period for the PIA and related policies and processes be agreed, funded, resources and conducted. This includes review of purpose, use, collection and annual system use audits, as well as destruction. Given that this project is a Proof of Concept, it's proposed that this be adopted if the project is scaled beyond the 12 months. Moreover, it's proposed that this be facilitated under existing procedures, frameworks and resourcing.
11	24	Seek advice on how to ensure non-LHD users are subject to minimum IT standards (inferred through Privacy Act and HRIP Act). Potentially use MOU or signed Ts and Cs.
12	25	That advice is sought on how patients should request access to their information held in Orion: use existing practices, or create an Orion-specific process. A request form may need to be added to the Orion project website. This information/process needs to be highlighted on the Orion project website, in the privacy section. Patient information policy: access, corrections,

		destruction, complaints.
13	26	That advice is sought on how patients should request access corrections to their information held in Orion: use existing practices, or create an Orion-specific process. A request form may need to be added to the Orion project website. This information/process needs to be highlighted on the Orion project website, in the privacy section. Patient information policy: access, corrections, destruction, complaints.
	27	Seek advice on whether the system be subject to current information management policies.
	28	Seek advice on who “owns” the system from a governance (information custodianship and accountability) perspective.
	29	Seek advice on how subpoena requests ought be managed.
	30	Seek advice on advising Medical Records of the existence of the system so that the system could be interrogated by Records in the event of a subpoena.
	31	Ensure training covers off access, corrections, destruction, complaints as well as privacy obligations, or that the information is on the website at a minimum.
	32	Subjecting the PIA, PIA response and PIA review to independent review such as the OAIC or NSW MOH Legal or NSW Government Legal. It is suggested that the Ministry of Health Legal and/or Privacy departments may sufficiently satisfy the “independent” test, and minimise cost in providing such review, for the purposes of the time-limited Proof of Concept. The Project Board and indeed LHD executive may view it prudent to engage an independent 3rd party review of the PIA in the event that the project is extended for wider use.

13 Conclusion

This PIA report demonstrates the project team are motivated to be accountable and transparent in their goal to protect and maintain individual persons' health information.

Whilst the system and project are materially compliant with key Australian Privacy Principles and the intent of privacy legislation in general, the project has made some recommendations to further strengthen privacy protections for patients.

The level of compliance of the system, coupled with the recommendations to further strengthen the privacy framework, should give comfort to the LHD Executive, Project Board, Project Partners and the Ministry of Health that the project has designed the system with privacy as a core tenet.

Overall this project is assessed to present a LOW privacy impact to patients and project partners.

14 Next steps

The privacy obligations of the project do not end with the issuing of this report.

It is recommended by the OAIC that the project and business respond to the report, identifying which recommendations it intends to implement in order to improve the privacy of patients.

A plan detailing how the accepted recommendations will be implemented would flow from that.

It is also recommended that the PIA (this document) be independently reviewed although this is not an obligation. Any review could be undertaken by the LHD Privacy Manager (already completed) in conjunction with the Orion Project Lead (for technical and project expertise). The OAIC or NSW Ministry of Health Legal/Privacy could also be invited to provide review feedback.

However, since this project is a Proof of Concept and not a broad scale deployment, an independent review is likely unnecessary, though this judgement is best-made by the Orion Project Steering Committee.

It is recommended that the PIA is reviewed with a view to influencing system design. However, since this PIA was completed quite late in the design and implementation stage, design changes will not materially change the information flows or general privacy considerations. Therefore, review may not be warranted until any system design augmentations are made after 12 months of operation.

15 Appendices

15.1 Appendix A

Table 15 Privacy and Access Model

Northern NSW	Care Plan *		Care Team Invite		Circle of Care		Goals & Actions			Goal Progress		Workflow Summary Assessments Patient Services Legal Documents Planned Appts Event Notes		Clinical Summary		Demographics	
	Read	Add/Edit	Read	Add/Edit	Read	Add/Edit	Read	Add	Edit	Read	Add/Edit	Read	Add/Edit	Read	Add/Edit	Read	Add/Edit
GP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Author	Yes	Yes	Yes	Yes	Yes	n/a	Yes	n/a
LHD Provider	Yes	x	Yes	x	Yes	x	Yes	Yes	Author	Yes	Yes	Yes	Yes	Yes	n/a	Yes	n/a
Private Provider	Yes	x	Yes	x	Yes	x	Yes	Yes	Author	Yes	Yes	Yes	Yes	Yes	n/a	Yes	n/a
Care Coordinator	Yes	x	Yes	x	Yes	x	Yes	Yes	Author	Yes	Yes	Yes	Yes	Yes	n/a	Yes	n/a
Practice Nurse	Yes	x	Yes	Yes	Yes	Yes	Yes	Yes	Author	Yes	Yes	Yes	Yes	Yes	n/a	Yes	n/a
Read only role	CDV tree	x	CDV tree	x	CDV tree	x	CDV tree	x	x	CDV tree	x	CDV tree	x	Yes	n/a	Yes	n/a
System Administrator	x	x	x	x	Yes	Yes	x	x	x	x	x	x	x	x	n/a	Yes	n/a