Best Start Kōwae
Privacy Impact Assessment Report

04 June 2020

Prepared by
Taria Tane, Project Manager National Hauora Coalition
## Document Summary

<table>
<thead>
<tr>
<th>Version</th>
<th>2.5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td>04/06/2020</td>
</tr>
<tr>
<td>Author</td>
<td>Taria Tane – National Hauora Coalition</td>
</tr>
<tr>
<td>Status</td>
<td>Approved – National Hauora Coalition Executive Leadership Team</td>
</tr>
</tbody>
</table>

## Document Version

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Reviewer Name/Title</th>
<th>Comments/Changes Requested</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/12/2019</td>
<td>1</td>
<td>Christine McIntosh/Clinical Advisor GEN2040</td>
<td>1.  Change wording re: arrangement between Procon &amp; Catalyst cloud</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2.  Widen scope to include entire Best Start Suite</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3.  Unify naming conventions</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4.  Consider access to data for evaluation/research</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5.  Consider wording re: de-identified data vs. encoded data.</td>
</tr>
<tr>
<td>21/01/2020</td>
<td>2.1</td>
<td>Tammy Dehar/ Privacy Officer National Hauora Coalition</td>
<td>1.  Include diagram to show pathway of patient information flow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2.  Wording updated on privacy responsibility of different entities at different stages</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3.  Create matrix to clearly show where responsibility for privacy lies at which stage.</td>
</tr>
<tr>
<td>02/03/2020</td>
<td>2.2</td>
<td>Darna Appleyard/Project Lead</td>
<td>1.  Restructure unanticipated risk reporting line to Governance Group.</td>
</tr>
<tr>
<td>04/03/2020</td>
<td>2.3</td>
<td>Dr Rawiri Jansen/Project Lead GEN2040</td>
<td>1.  Rename: Best Start – Pregnancy assessment tool.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2.  Info flow diagram: PHO receive performance data</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3.  Include NHC in the Data stakeholder table</td>
</tr>
<tr>
<td>04/03/2020</td>
<td>2.3</td>
<td>National Hauora Coalition Executive Leadership Team</td>
<td>Approved.</td>
</tr>
<tr>
<td>14/04/2020</td>
<td>2.3</td>
<td>Office of Privacy Commissioner</td>
<td>Commentary/feedback can be provided upon request. All suggestions made by the Office of Privacy Commissioner have been incorporated into version 2.4, including: 1. Clarifying project timeframes and storage timeframes 2. Implementing review from external stakeholder 3. Insert Health Information Privacy Code (1994) legislation and responses to rules 4. Detailing of privacy risks, who these risks impact, and what might happen if risks were to occur 5. Planning for breaches 6. More specificity for the purposes of collection of information and use 7. More clarity regarding information pulled from PMS and why it is necessary to do this 8. Reference Retention of Health Information (1996) legislation 9. Detailing how we are disposing of information who makes decision regarding disposal 10. Clarity regarding agency responsibilities and boundaries 11. More details regarding purpose and function of Māori data governance group 12. More details regarding monitoring and review plan for PIA</td>
</tr>
</tbody>
</table>
3. Provide clarity on how patients will know they are participating in Best Start Kōwae. Suggest to add notification for consent/decline. (in progress)

04/06/2020 2.5 Finalised Report

### Abbreviation List

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BCTI</td>
<td>Buyer Created Tax Invoice</td>
</tr>
<tr>
<td>CRA</td>
<td>Cloud Risk Assessment</td>
</tr>
<tr>
<td>EPAT</td>
<td>Early Pregnancy Assessment Tool</td>
</tr>
<tr>
<td>Gen2040</td>
<td>Generation 2040 Project</td>
</tr>
<tr>
<td>GP</td>
<td>General Practitioner</td>
</tr>
<tr>
<td>HIPC</td>
<td>Health Information Privacy Code (1994)</td>
</tr>
<tr>
<td>LMC</td>
<td>Lead Maternity Carer</td>
</tr>
<tr>
<td>MOH</td>
<td>Ministry of Health</td>
</tr>
<tr>
<td>NHC</td>
<td>National Hauora Coalition</td>
</tr>
<tr>
<td>NHI</td>
<td>National Health Identifier</td>
</tr>
<tr>
<td>PCP</td>
<td>Primary Care Provider</td>
</tr>
<tr>
<td>PHO</td>
<td>Primary Health Organisation</td>
</tr>
<tr>
<td>PIA</td>
<td>Privacy Impact Assessment</td>
</tr>
<tr>
<td>PMS</td>
<td>Practice Management System</td>
</tr>
<tr>
<td>PSAAP</td>
<td>PHO Services Amendment Agreement Protocol</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Socket Layer</td>
</tr>
</tbody>
</table>
# Table of Contents

1. **Introduction** .................................................................................................................. 5
2. **Scope and Process** ......................................................................................................... 8
3. **Information Flows and Personal Information** .............................................................. 10
   4.1. Principle 1 – Purpose of the collection of personal information .................................. 22
   4.2. Principle 2 – Source of personal information ............................................................... 24
   4.3. Principle 3 – Collection of information from subject ................................................... 25
   4.4. Principle 4 – Manner of collection of personal information ......................................... 27
   4.5. Principle 5 – Storage and security of personal information ......................................... 28
   4.6. Principle 6 – Access to personal information ............................................................... 30
   4.7. Principle 7 – Access to personal information ............................................................... 31
   4.8. Principle 8 – Accuracy of personal information ........................................................... 32
   4.9. Principle 9 – Not to keep personal information for longer than necessary .................. 33
   4.10. Principle 10 – Limits on use of personal information .................................................. 34
   4.11. Principle 11 – Limits on disclosure of personal information ....................................... 35
5. **Risk Management** ......................................................................................................... 37
   5.3. Unanticipated Risk Management Strategy .................................................................... 41
   5.4. Privacy Breach Response Plan .................................................................................... 42
6. **Conclusion** ....................................................................................................................... 42

Appendix A. Supporting Documents ................................................................................... 43
1. Introduction

1.1. Background

Primary care has long struggled with providing comprehensive, consistent best practice assessment and management at the early pregnancy consult and at the six week postnatal infant check. There is significant unrealised opportunity to address inequity in access and improve quality of care across all stages of pregnancy and thereby reduce disparity in health outcomes for mothers and babies.

The National Hauora Coalition has recently been awarded funding via the Ministry of Health and Primary Health Organisation (PHO) Services Amendment Agreement Protocol (PSAAP) to lead the national roll out of a suite of pregnancy assessment tools/modules (also called Best Start Kōwae) in Primary Care, as part of a wider pro-equity project called ‘Generation 2040’ (Gen2040). The Gen2040 project will provide incentive payments for use of the Best Start Kōwae (assessment modules) with Māori Hapū Māmā (pregnant women) and Pēpī Māori (Māori babies). The goal of the Gen2040 project is to improve access to quality care and wrap around support in Primary Care for all women, with a particular focus on improving outcomes for Māori.

The Best Start Kōwae will be developed working collaboratively with the providers with whom the mother and infant will interact with in her pregnancy and early infancy journey (General Practice and Midwifery), to ensure a more collaborative, virtual care team approach. The assessment modules will predominantly interface with practice management systems, however a secure online webform version of the tools will also be available for use. There will be up-to-date, localised, evidence-based clinical support embedded in all of the Best Start Kōwae.

1.1.1. Project Timeline

As of March 2020, the Gen2040 project has been funded to run from December 2019 to December 2020. The project involves the national rollout of the Best Start Kōwae, a suite of assessment available for use by Primary and Maternity Care Providers. In light of the current COVID-19 pandemic, the Gen2040 project may extend beyond December 2020.

1.1.2. What are the Best Start – Pregnancy Assessment Tools?

The Best Start Kōwae include:

- Best Start – Pregnancy Tool
  - Status: Developed; Piloted; Security testing completed; awaiting go live.

- Best Start – Pregnancy 16 Week Check
  - Status: Under development

- Best Start – Pregnancy 6 Week Māmā
  - Status: Pre-development

- Best Start – Pregnancy 6 Week Pēpī
  - Status: Pre-development
1.1.3. Who will use the Best Start Kōwae?

Each of the Best Start assessments will be rolled out on a nationally across Aotearoa and will be available for use by primary and maternity care providers (e.g., General Practitioners, nurse practitioners, nurses, Lead Maternity Carers, Midwives etc). The Best Start Kōwae will be embedded in most practice management systems (PMS) and will also be available via secure online web-based form (LMC access/GP where the Best Start Kōwae cannot interface with PMS).

1.1.4. How the Best Start Kōwae are used across the pregnancy journey

Best Start – Pregnancy Tool

The Best Start -Pregnancy Tool is completed at confirmation of pregnancy consultation with either primary or maternity care providers, which typically occurs within the first 12 weeks of pregnancy. There are no time limits on when this assessment can take place (i.e., if a pregnant woman confirms pregnancy at 24 weeks, she can still have the assessment done). Providers will complete the assessment via a verbal, in-person consultation with the pregnant woman.

Best Start – Pregnancy 16-Week Check

Providers will have the ability to recall patients at 16- weeks for a follow up consultation focusing on pertussis and flu vaccinations, as well as support service utilisation. Healthcare providers will complete the tool via a verbal, in-person consultation with patients.

Best Start – Pregnancy Enhanced 6 Week Check (Māmā)

Healthcare providers (GP or LMC) will complete a comprehensive 6 week post-partum check on all mother’s as part of a handover consultation from LMC to Primary Care. Healthcare providers will complete the tool via a verbal, in-person consultation with patients.

Best Start – Pregnancy Enhanced 6 Week Check (Pēpī)

Healthcare providers (GP or LMC) will complete a comprehensive 6 week post-partum check on all babies, as part of a handover consultation from LMC to Primary Care. Healthcare providers will complete the tool via a verbal, in-person consultation with patients.

1.1.5. How often will patients complete a Best Start – Pregnancy Assessment?

There will be 3 official “touch-points” over the pregnancy journey, where patients will be asked to complete a Best Start – Pregnancy Assessment.

1.1.6. What will happen with personal information?

For the purpose of this PIA, we distinguish the use of personal information into two categories.

1.1.6.1. To support Best Start Kōwae Functionality

Personal information will be collected in each of the Best Start Kōwae for the following purposes:

- For storage in a secure cloud-based server. This will facilitate cross-sector integration of the Best Start Kōwae. This means providers from different sectors (i.e., maternity vs. primary) have the ability to update assessments. For example, if a GP completes a Best
Start Pregnancy and submits the form, the patient’s midwife will have the ability to view and update the same assessment.

- To support decision support functionalities built into the tool. Evidence-based decision support algorithms are built into the Best Start Kōwae and require the input of personal information to enable these decision support functionalities.

1.1.6.2. To fulfil Gen2040 Project requirements

Personal information is collected for the purpose of fulfilling Gen2040 clinical outcome reporting and payment requirements, including:

- Personal information is needed to complete and provide incentive payments to providers completing the Best Start Kōwae with Māori hapū māmā and pēpī Māori (i.e., NHI, date of assessment completed, name of assessment)
- To facilitate anonymised clinical and equity-related outcome reporting to PHO’s, providers using the tools, our funder (Ministry of Health), programme evaluators and internal researchers.

1.1.7. Why is a Privacy Impact Assessment (PIA) needed?

Patients care how their information is handled and the Generation 2040 project will hold potentially identifiable patient information by design (in order to provide the benefits it does). By managing privacy successfully and showing how we take care of personal information, the Gen2040 project will be able to provide a better service and will meet patient needs around information sharing that enables their health and social care.

This PIA will help identify potential areas of risk that may breach privacy and outline the strategies used in this project to mitigate those risks. Additionally, this PIA will provide assurance to internal and external stakeholders of the considerations around risk and compliance with Privacy Act 1993 and Health Information Privacy Code 1994 principles (described in more detail below).

The production of this PIA in these early stages of tool development will allow the Generation 2040 project to identify and address any early privacy issues or concerns. This PIA has been reviewed by the Office of Privacy Commissioner. Once this the PIA has been finalised, a final report will be published and available via the Generation 2040 website.

1.1.8. PIA review plan

This PIA will be updated if there are any deviations from the scope or any changes that impact how we respond to any of the privacy principles described in this current document version. Any updated PIA’s will be reviewed by the contributors and reviewers stated below. The Gen2040 Data Analyst will be responsible for monitoring our practice against this PIA. A wider privacy review will be conducted by the Gen2040 Māori Data Governance group on a 6-monthly basis until project completion.
2. Scope and Process

2.1. Scope

This PIA will cover the following systems and products:

- IT Infrastructure (cloud-based webforms; cloud-based Procon-hosted server; NHC server)
- Data transference from Practice Management Systems
- Data transference from webforms
- Information management (including use, storage, access, retention and disposal)
- Handling personal information and risk management strategies

This PIA does not cover the use of personal information by providers who use the Best Start Kōwae.

A Cloud Risk Assessment and penetration testing has been completed as part of the security and privacy review process.
2.2. Contributors

This PIA (Version 2.5) was developed by the current Generation 2040 Project Manager in consultation with the below key stakeholders. The draft PIA will be shared with the below key stakeholders for comments and suggestions before a final version is published.

<table>
<thead>
<tr>
<th>Name</th>
<th>Role</th>
<th>Organisation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dr Christine McIntosh</td>
<td>Clinical Advisor</td>
<td>Child Health, Primary &amp; Integrated Care (Counties Manukau DHB)</td>
</tr>
<tr>
<td>Ken Leech</td>
<td>Chief Executive Officer/ IT developer of the EPAT</td>
<td>Procon Limited</td>
</tr>
<tr>
<td>Jonathan Murray</td>
<td>Group Manager – Primary Health Services &amp; Mōhio Services/Mōhio lead</td>
<td>National Hauora Coalition</td>
</tr>
<tr>
<td>Rawiri Mckree Jansen</td>
<td>Project Director – Gen2040</td>
<td>National Hauora Coalition</td>
</tr>
<tr>
<td>Tammy Dehar</td>
<td>Privacy Officer – National Hauora Coalition</td>
<td>National Hauora Coalition</td>
</tr>
<tr>
<td>Office of Privacy Commissioner</td>
<td>N/A</td>
<td>Office of the Privacy Commissioner</td>
</tr>
<tr>
<td>Health Quality &amp; Safety Commission</td>
<td>N/A</td>
<td>Health Quality &amp; Safety Commission</td>
</tr>
</tbody>
</table>

2.3. Process

The following activities will be undertaken prior to publishing this PIA:

- Draft preparation of PIA
- Draft distributed to reviewers for feedback
- Feedback incorporated
- Interim report published
- Independent review conducted by Office of Privacy Commissioner
- Feedback incorporated
- Final report prepared and published
- Final report made available via NHC website
3. Information Flows and Personal Information

3.1. Information Flows

The Best Start Kōwae will be embedded in PMS and available via secure online webform. Figure 1. shows the end-to-end flow of personal information.

**Best Start PMS**

If the Best Start Kōwae are accessed via PMS, each tool will have the ability to pull and pre-fill historical clinical information directly into the tool from the PMS. This is intended to create efficiencies in assessment completion with patients.

**Best Start Online**

The Best Start Kōwae will also be made available via secure online web-based forms. Health Providers will be allocated secure logins by the Gen2040 Project team. A Best Start Online Access Application process will be initiated to check clinical credentials prior to access being given. This process will be managed by the Gen2040 project team. Historical clinical information will not be pre-filled in the web-based form (as there are no linkages to a PMS to be able to do this). However, if an assessment is completed first using the Best Start PMS version and later completed via Best Start Online, the information saved in the Best Start PMS version will be pulled across to Best Start Online and stored on a secure Catalyst cloud-based server.
Generation 2040 Privacy Impact Assessment

Figure 1. Personal Information Flow

- **Primary Care – GP/Nurse**
  - Practice Management System (PMS)
    - Access to Best Start Kōwae
    - Referrals/recalls via Best Start
    - Some clinical information pulled through to Best Start tool
    - Summary of care

- **Hapū Māmā**

- **LMC/Other Health Care Provider**

- **Best Start Online**
  - Access to Best Start Kōwae for LMC/Other Health Providers via secure login
  - No connection to PMS
  - Access via URL
  - Bi-directional feed

- **Best Start PMS**
  - Access to Best Start Kōwae for PCP (nurse/GP)
  - Bi-direction feed with PMS
  - Access via advanced forms in PMS

- **Catalyst Cloud-based Server**
  - Stores patient information collected from Best Start Kōwae
  - Hosts decision support/referrals management system

- **Generation 2040 Project**
  - Administration
  - Outcome reporting (Māori only)
  - Incentive payment administration and reporting

- **Primary Health Organisations**
  - Receives clinical outcome reporting
  - Receives incentive payments for distribution to GP network
  - Receives incentive payment reporting
  - Performance data reporting

Note: If a health professional (HP) completes PMS version of any Best Start Kōwae and saves/submits, the data pulled across to the Best Start tool from the PMS will be saved on the cloud-based server. If a HP later accesses the online version of the Best Start tool, the data pulled across from the PMS will be saved and will show in the online version of the tool.
3.2. Procon Limited

3.2.1. Background

Procon Limited has been providing software solutions in the health sector since 2007 and specialises in tools that integrate with the practice management systems used within primary care. Procon has recently been commissioned by Counties Manukau DHB to provide a SUDI risk calculator that is being used by midwives within the hospital setting to assess the SUDI risk of women who are admitted within the maternity ward and to refer these women to appropriate services that will reduce the risk. Procon was then subsequently invited to propose its services to develop the Best Start – Pregnancy Assessment EPAT that is part of the Gen2040 project.

Procon software designer Ken Leech has local expertise in designing cloud based tools for patient information and referral management systems for DHB’s and Primary care. Prior software developed by Procon for programmes using the same server have undergone PIA, Cloud Risk assessment (CRA), and is in currently in clinical use.

3.2.2. Physical Access and Location

The server that hosts the Best Start PMS and database is externally hosted by Catalyst Cloud with the physical server accessible only to Catalyst Cloud administrators. The servers are physically located in their data centres in Hamilton, Porirua and Wellington. Procon itself has no access to the physical server.

3.2.3. Operating System Access and Maintenance

Procon has a service level agreement in place with Catalyst Cloud to access and maintain the server on behalf of Procon Limited. This agreement includes monthly patching and all operating system upgrades as required.

3.2.4. Database Access

All Best Start Kōwae data will be held within a MySQL database on the secure server. Authorised Procon employees will have access to the database where personal information will be stored. All other access is provided under application software control. No immediately identifiable personal information (i.e., first name, last name, address) will be transferred across to the server. Personal information will be de-identified using National Health Identifier (NHI) as an ID. Information that could identify a patient is encrypted at the database level.

3.2.5. Best Start Online - Application Access

The online application is accessible to anyone who is connected to the Internet (as access needs to be provided to users who may need to access the application from external and unpredictable locations). All access is via https protocols and requires a login with user name and strong password. Standard processes are in place to allow users to reset their passwords should this be required.

3.2.6. Personal Information Accessed
Catalyst cloud-based servers will store all personal information collected via the Best Start Kōwae, for both PMS and Online versions.

### 3.3. National Hauora Coalition IT Platform

#### 3.3.1. Background

Mōhio is an IT platform owned by the National Hauora Coalition and used in the day-to-day operations of our organisation that involves the routine and ongoing collection of patient medical, financial, demographic and other personal identifiable data.

The Mōhio Platform currently works in conjunction with other existing software such as a General Practice’s Practice Management Systems (PMS) or stand-alone to assist in the management and storage of patients’ individual information including: clinical, demographic, financial, utilisation and other personal data. A PIA has previously been completed for the Mōhio platform and is currently being penetration tested. Results of the final Penetration Test Report will be made available upon request.

#### 3.3.2. Physical Access and Location

Mōhio is hosted and its databases are stored in two New Zealand based data centres, on dedicated servers, with appropriate physical security and access in place. The NHC’s Mōhio system runs on a Windows server hosted within New Zealand or Microsoft Azure hosted in Australasia, which was approved by the New Zealand Ministry of Health in July 2016 for storage of personal health data.

#### 3.3.3. Operating System Access and Maintenance

The secure Mōhio servers are only accessed by authorised personnel. Security patching is applied according to best practice.

#### 3.3.4. Database Access

Direct databases access is limited to very few users who are required access for ongoing development and maintenance.

#### 3.3.5. Application Access

Unique logins and passwords are issued for each Mōhio user. Role based security profiles ensure that only authorised users have access to limited part of system, including subsets of de-identified patient information collected as part of the Gen2040 Project. Logins and activity on the system to the system are logged for audit purposes.

#### 3.3.6. Personal Information Accessed

As part of the Gen2040 project, Mōhio servers will access all clinical data submitted in a Best Start Kōwae where an ‘Active pregnancy’ is indicated; and the pregnant woman identifies her baby’s ethnicity as ‘Māori’. The personal information accessed by Mōhio servers will be de-identified by National Health Identifier (NHI).
3.4. Personal Information

3.4.1. Why we collect and retain personal information for the Gen2040 Project

As part of the Gen2040 project, Mōhio servers will access all clinical data submitted in a Best Start – Pregnancy Assessment where an ‘Active pregnancy’ is indicated; and the pregnant woman identifies her baby’s ethnicity as ‘Māori’. Patient’s de-identified (via NHI) clinical, demographics, utilisation and other personal data will be collected and retained for the purpose of:

- Better identifying population needs
- Clearly identify inequities and ethnic/quintile breakdowns
- Creating practice-level pregnancy registries
- Evaluating and monitoring performance of health services
- Feedback to PHO’s, funders and external stakeholders
- Facilitating accurate and efficient Buyer Created Tax Invoice (BCTI) payments
- Improving quality through data informed clinical governance
- Improving the capability to manage and monitor contractual agreements
- Managing claims and billing (including auditing)
- Meeting Ministry of Health and District Health Board requirements for provision of information under contractual and legislative requirements
- More effectively assessing if what we do is making a difference to health outcomes
- More effectively collaborating to remove barriers in achieving best care
- Reducing administrative waste and duplication of effort in the system
- Reducing cost in time and resources for data collection and submission
- Reducing duplication of effort by enabling data to be captured once and then be securely and appropriately seen where and when it is needed
- Support best practice evidence for clinical interventions

3.4.2. Types of Personal Information Collected

Currently, Gen2040 has only developed the first of te Best Start Kōwae, called the Best Start – Pregnancy Tool. A snapshot of the data fields in the Best Start – Pregnancy Tool have been included below to provide a detailed account of the types of personal data collected and retained as part of the Gen2040 project.

3.4.2.1. New Pregnancy

- Pregnancy status
- Confirmation type (Urine BHCG; Serum BHCG)
- Assisted pregnancy and assistance given
- Date of LMP
- Estimated delivery date
- Periods
- Response to pregnancy news (Positive; Unsure; Considering adoption or whāngai; Considering termination)
- Ethnicity & Iwi
- Early pregnancy problems (Vaginal bleeding; Low abdominal pain; Nausea/vomiting; UTI; Trauma; IUCD In Situ)
3.4.2.2. Obstetric History
- Gravida and Parity
- First pregnancy with current partner
- Record of previous births (Baby’s first name; Year born; gender; Ethnicities of the baby; Gestation; Multiple birth; Birth method; Weight; Outcome; Complications)

3.4.2.3. Medical History
- Any past or ongoing medical problems (e.g., Diabetes; Infectious diseases; Neurological)
- Personal or family genetic conditions (e.g., Sickle cell anaemia; Cystic fibrosis)
- Experienced any mental health problems
- Depression screening (PHQ)
- Anxiety screening (GAD)

3.4.2.4. Wrap around support
- Whānau support
- Smoking status (mother and household smoking)
- Alcohol use
- Drug use
- Housing
- Intimate partner violence
3.4.2.5. Examination and Screening
- Blood Pressure
- Heart Sounds
- BMI
- Abdominal/pelvic examination
- Respiratory
- Cervical screen status
- Sexually Transmitted Infection examination and testing
- Routine screening
- First/Second semester combined screening

3.4.2.6. Prescriptions
- Medication review (long term or prescribed in last 6 months)
- Use of supplements or alternative medications
- Use of Rongoā or other cultural traditional healing practices?
- Use of folic acid, reasons for high dose folic acid
- Folic acid prescribed at consultation
- Use of iodine & prescription
- Aspirin indication and reason for aspirin indication
- Calcium indication
- Vitamin-D indication

3.4.2.7. Vaccinations
- Influenza vaccination given/recall
- Pertussis (Whooping Cough) vaccination
3.4.2.8. Care Planning
- Choice of birthing location
- Maternity care options
- Post-partum contraception options
- Healthy diet and weight
- Food preparation

3.4.2.9. Action Summary
- Displays advice and checklist actions for any relevant areas requiring appropriate follow up.

3.5. Privacy Responsibility and Privacy Boundaries
3.5.1. National Hauora Coalition

Although the National Hauora Coalition is leading the national roll out of the Best Start Kōwae as part of the Gen2040 project, implementation of the tools involves external health organisations who are responsible for how they manage privacy. The National Hauora Coalition will mitigate any organisational privacy risks via a ‘Provider Service Agreement’ (See Appendix A. Provider Service Agreement) which stipulates adherence to the Privacy Act 1993 and Health Information Privacy Code 1994 in the conduct and use of the Best Start Kōwae. It is important to outline organisational responsibilities for privacy and privacy boundaries (see Figure 2).

The National Hauora Coalition will be responsible for Privacy relating to:

- How privacy is managed by their IT vendor (Procon Limited);
- Access, use and storage of personal information by the National Hauora Coalition; and
- Transference of personal information between PHO’s/maternity care providers/primary care providers (see ‘National Hauora Coalition’ Privacy Boundary in Figure 2).
- Privacy responsibilities between the National Hauora Coalition and PHO’s/maternity care providers/primary care providers are outlined in ‘Provider Service Agreement’ (See Appendix A. Provider Service Agreement).
3.5.2. **Primary Health Organisations/PCP/LMC/Other Health Providers**

Privacy matters relating to PMS and clinical care between patients and their health professionals is outside the scope of this PIA, as it is the health professional’s individual responsibility to protect patient information as part of their clinical care. The handling of privacy will therefore be at the discretion of those entities and individual health professionals (see ‘Primary Health Organisations/PCP/LMC/Other Health Provider’s’ boundary label in Figure 2). Because the National Hauora Coalition will provide personal information to PHO’s, a clause on privacy and privacy responsibility of each PHO has been included in ‘Provider Service Agreement Service Specifications’ (See Appendix A. Provider Service Agreement).

3.5.3. **Procon Limited**

Procon Limited will be responsible for privacy matters relating to:

- IT security factors associated with privacy;
- The transference of personal information between PMS to Catalyst cloud-based Server;
- Transference of personal information between patient to Best Start Online to Procon-hosted Server;
- Access of personal information; and
- Storage of personal information on Catalyst cloud-based Server.

Privacy responsibilities will be outlined in contractual agreement between Procon and The National Hauora Coalition.
Figure 2. Privacy Responsibilities and Privacy Boundaries

Privacy Boundaries Key
- National Hauora Coalition
- Procon Limited
- Primary Health Organisations/PCP/LMC/Other Health Providers

Referral to localised support services
Localised decision support
Best Start Pregnancy Tools
Secure Online URL
Catalyst Cloud-Based Server
Primary Care Provider (PCP)
Lead Maternity Carer (LMC)/Other Health Providers
Primary Health Organisations
Payments and BCTI Reporting
NHC Server
Māori only
All data captured in tools
Localised decision support
Best Start Pregnancy Tools
Secure Online URL
Catalyst Cloud-Based Server
Primary Care Provider (PCP)
Lead Maternity Carer (LMC)/Other Health Providers
Primary Health Organisations
Payments and BCTI Reporting
NHC Server
Māori only
All data captured in tools
Localised decision support
Best Start Pregnancy Tools
Secure Online URL
Catalyst Cloud-Based Server
Primary Care Provider (PCP)
Lead Maternity Carer (LMC)/Other Health Providers
Primary Health Organisations
Payments and BCTI Reporting
NHC Server
Māori only
All data captured in tools
Localised decision support
Best Start Pregnancy Tools
Secure Online URL
Catalyst Cloud-Based Server
Primary Care Provider (PCP)
Lead Maternity Carer (LMC)/Other Health Providers
Primary Health Organisations
Payments and BCTI Reporting
NHC Server
Māori only
All data captured in tools
Localised decision support
Best Start Pregnancy Tools
3.6. Access to Personal Information

Mōhio has a secure online reporting system that will be used as the Gen2040 reporting portal. This portal will be restricted to appropriate user access rights by the Gen2040 Data Analyst. The reporting portal can be accessed through an internet browser. Alternative data reports can be created and provided to approved users via the Gen2040 Data Analyst. All reports containing patient-level personal information will be password protected and user access restricted. The following access to personal information reported by the Gen2040 project is proposed:

<table>
<thead>
<tr>
<th>Information</th>
<th>Data level</th>
<th>Stakeholder Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Best Start Kōwae PDF Printout of results</td>
<td>Individual</td>
<td>X Patient</td>
</tr>
<tr>
<td></td>
<td></td>
<td>X Practice</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NHC</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PHO</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DHB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MoH</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Evaluators/researchers</td>
</tr>
<tr>
<td>Best Start Kōwae data (de-identified)</td>
<td>Individual – De-identified Māori data</td>
<td>Patient</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Practice</td>
</tr>
<tr>
<td></td>
<td></td>
<td>X NHC</td>
</tr>
<tr>
<td></td>
<td></td>
<td>X PHO</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DHB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MoH</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Evaluators/researchers</td>
</tr>
<tr>
<td>BCTI Payment Reporting</td>
<td>Practice Level - De-identified Māori data</td>
<td>Patient</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Practice</td>
</tr>
<tr>
<td></td>
<td></td>
<td>X NHC</td>
</tr>
<tr>
<td></td>
<td></td>
<td>X PHO</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DHB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MoH</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Evaluators/researchers</td>
</tr>
<tr>
<td>Outcome Reporting PHO</td>
<td>Practice Level (within PHO Network)</td>
<td>Patient</td>
</tr>
<tr>
<td></td>
<td></td>
<td>X Practice</td>
</tr>
<tr>
<td></td>
<td></td>
<td>X NHC</td>
</tr>
<tr>
<td></td>
<td></td>
<td>X PHO</td>
</tr>
<tr>
<td></td>
<td></td>
<td>X DHB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>X MoH</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Evaluators/researchers</td>
</tr>
<tr>
<td>Outcome Reporting MoH</td>
<td>National + PHO + Practice Level</td>
<td>Patient</td>
</tr>
<tr>
<td></td>
<td></td>
<td>X Practice</td>
</tr>
<tr>
<td></td>
<td></td>
<td>X NHC</td>
</tr>
<tr>
<td></td>
<td></td>
<td>X PHO</td>
</tr>
<tr>
<td></td>
<td></td>
<td>X DHB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>X MoH</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Evaluators/researchers</td>
</tr>
<tr>
<td>Other Outcome Reporting</td>
<td>National + PHO + Practice Level</td>
<td>Patient</td>
</tr>
<tr>
<td></td>
<td></td>
<td>X Practice</td>
</tr>
<tr>
<td></td>
<td></td>
<td>X NHC</td>
</tr>
<tr>
<td></td>
<td></td>
<td>X PHO</td>
</tr>
<tr>
<td></td>
<td></td>
<td>X DHB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>X MoH</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Evaluators/researchers</td>
</tr>
<tr>
<td>De-identified Māori data</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
3.7. Security Measures

3.7.1. Māori Data Governance

Data Governance refers to a key business activity that utilises the skillset of an expert group (Data Governance Group) and procedures that build and maintain confidence in the information and decision support captured and reported as part of the Generation 2040 project. In particular, Data Governance provides:

- Transparency and trust in data management processes, information and the Generation 2040 decision support evidence-base; and
- Expert guidance over data practices, quality, and mitigation of risks and issues.

The Gen2040 project has recently formed a Māori Data Governance Group, which will be responsible for ensuring the proper handling of Māori data, exercising tino rangatiratanga sovereignty under Te Tiriti o Waitangi obligations. The Māori Data Governance Group is comprised of Māori health experts and will be responsible for activities such as:

- Reviewing and approving policies associated with collecting, accessing, using and retaining data obtained via the Best Start Kōwae
- Providing expertise over risk management procedures
- Ensuring regulatory compliance
- Ensuring Māori data is appropriately handled
- Contributing to data quality measures
- Providing expert advice regarding data breaches
- Guiding data strategy and data priorities;
- Monitoring compliance with data standards, policies and legislation;
- Providing expert guidance on data issue resolution, security, protection, access and management; and
- Ensuring data management processes are ethical and fit-for-purpose

3.7.2. Service Agreements

Procon Limited and PHO’s/LMC’s/Other Health Providers will be engaged via Service Agreements prior to the rollout of the Best Start Kōwae. These Service Agreements will outline privacy responsibilities relating to the Best Start Kōwae and Gen2040 project.

3.7.3. Penetration Testing

As an additional precaution, the National Hauora Coalition is currently undergoing a penetration test by ZX Security on Procon and Mōhio Servers as part of the Gen2040 project implementation plan. Once completed, the results of the final penetration testing report will be made available to stakeholders upon request.

3.7.4. Internal Auditing and Data Checking

The Gen2040 Project Team will conduct regular data checking and audits on the Mōhio system as part of data quality improvement activities over the project lifecycle.

Each of the twelve Privacy Principles encompassed in the Privacy Act 1993 are headlined using a brief summary of each rule; the full wording for each rule is readily available online from the Privacy Commissioner¹.

The Health Information Privacy Code (HIPC) 1994 regulates how health agencies (such as doctors, nurses, pharmacists, health insurers, Primary Health Organisations and District Health Boards) collect, hold, use and disclose health information about identifiable individuals. The HIPC applies to all health agencies in the health sector. Please note: typically, the HIPC replaces the Privacy Act.

For the purposes of this PIA, both the Privacy Act and HIPC principles will be acknowledged and addressed.

Other relevant applicable legislation adhered to includes:

HISO 10029:2015 Health Information Security Framework
New Zealand Information Security Manual
New Zealand Government Protective Security Requirements

4.1. Principle 1 – Purpose of the collection of personal information.

Privacy Act Principle 1 - Purpose of the collection of personal information.
Only collect personal information if you really need it

HIPC Rule 1 - Only collect health information if you really need it.

The collection is for a lawful purpose, connected with what the agency does, and it is necessary to collect the information for that purpose.

4.1.1. Why we are collecting personal information

The National Hauora Coalition (host organisation for the Gen2040 project) is a Primary Health Organisation who handles personal health information as part of its business function.

Personal health information is collected to fulfil the requirements of the Gen2040 project and to fulfil functionality requirements within the tool.

To fulfil functionality requirements of the Best Start Kōwae

• The Best Start Kōwae has a built-in decision support function that supports providers to give best practice clinical advice. To achieve this function, the Best Start Kōwae uses algorithms based on clinical information input. We therefore require the collection and storage of clinical information.

• When an assessment form is submitted, providers have the ability to open and update information in the form. The updated information is stored in the cloud-based server.

**For the purpose of required Gen2040 project reporting:**

Gen2040 uses an incentive-based approach to identify and address inequities in maternity care for Māori. There are major gaps in literature and evidence relating inequities in maternity care. We therefore will collect personal information that will help us identify and address inequities and clinical outcomes in our reporting to funders, PHO’s, researchers and project evaluators. We also collect personal information to provide:

• Clinical outcome and payment reporting to PHO’s regarding Māori hapū māmā within their networks;

• Clinical outcome and payment reporting to our funders (MoH) and for project evaluation purposes; and

• To calculate and produce incentive payments for providers using the tool.

### 4.1.2. Personal information we are collecting

• All de-identified (by NHI) personal information logged in each Best Start Kōwae for non-Māori will remain within the cloud-based server.

• All de-identified (by NHI) personal information logged in each Best Start Kōwae for Māori hapū māmā and pēpī Māori will be accessed by the Gen2040 project team for the purposes described above.

  o Our base criteria for collecting information:

  • Pregnancy identified as “Active” AND

  • Mother’s ethnicity identified as “Māori” OR

  • Ethnicity of the baby is identified as Māori

### 4.1.3. Personal information we are not collecting.

**For the purposes of the Gen2040 project**

We will not be collecting any personal information from mothers or babies who are indicated as non-Māori. All personal information from non-Māori collected in the Best Start Kōwae will remain in a secure database hosted by our vendor Procon. The National Hauora Coalition will not have access to this personal information.

Procon will maintain responsibility for the storage and security of all personal information stored in their cloud-based server.

We may request collect a summary statistic from Procon regarding number of assessments completed with Non-Māori, so we are enabled to report comparisons. This is important for identifying any equity gaps that may be present.

### 4.1.4. Assessment of compliance
The purpose of collection is lawful and connected with the function of the agency and project. We are collecting personal information to support best practice clinical care and meet Gen2040 project requirements.

4.1.5. Risk Assessment

The risk of this principle being breached is low.

4.2. Principle 2 – Source of personal information

<table>
<thead>
<tr>
<th>Privacy Act Principle 2 – Source of personal information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get it directly from the people concerned wherever possible</td>
</tr>
</tbody>
</table>

**HIPC Rule 2 - Health information must usually be collected from the person the information is about. But sometimes it is all right to collect information from other people instead - for instance, when:**

- Getting it from the person concerned would undermine the purpose of the collection
- It’s necessary so a public sector body can uphold or enforce the law
- The person concerned authorises collection from someone else

4.2.1. How we collect personal information

**Directly from the hapū māmā**

Where possible and appropriate, personal information will be collected via direct verbal communication between a health provider and their patient.

**Practice management systems**

In some instances, it is more appropriate to collect information directly from the PMS. Instances include the collection of some clinical information (e.g., blood pressure readings in the last 12 months), as this information is based off historical measurement results and is stored within the PMS. This method will only be applicable for the PMS versions of the Best Start Kōwae.

4.2.2. Assessment of compliance

Where appropriate and possible, personal information be collected directly from the patient. In some instances it is more appropriate to collect personal information directly from the PMS, to remove the risk of human error (e.g., the patient providing incorrect details or not being able to recall clinical details).

By consenting to enrolling as a patient with their general practice, patients are asked to consent to their personal information relevant to a programme in which they may be enrolled in (in this case – Best Start Kōwae) to be sent to the PHO or the external health agency managing the programme (see Appendix A. PSAAP Enrolment Toolkit for PHO’s).
4.2.3. Risk Assessment

Given that we have a justified reason for collecting information from PMS, the risk of this principle being breached is low.

4.3. Principle 3 – Collection of information from subject

Principle 3 – Collection of information from subject

Tell them what information you are collecting, what you’re going to do with it, whether it’s voluntary, and the consequences if they don’t provide it.

When a health agency collects health information from the person the information is about, it has to take reasonable steps to make sure that person knows things like:

- Why it is being collected
- Who will get the information
- Whether the person has to give the information or whether this is voluntary
- What will happen if the information isn’t provided

Sometimes there are good reasons for not letting a person know about the collection, for example, if it would undermine the purpose of the collection, or it’s just not possible to tell the person.

4.3.1. What the patient will know or be told

- The Best Start Kōwae are assessment tools to facilitate best practice clinical care in New Zealand. It is therefore the decision of the primary or maternity care provider to offer to use the Best Start Kōwae with their patients.
- Completion of the Best Start Kōwae is voluntary (for the clinician and the patient). Patients reserve the right to decline completing the Best Start Kōwae. There will be no consequences or negative impact to the patients’ clinical care, should they decline to have any of the Best Start Kōwae completed.
- As mentioned above, patients will not be asked for written informed consent regarding their data being collected for the purpose of the Gen2040 project (Māori Māmā and Pēpī Māori only). By consenting to enrolling as a patient with their general practice, patients are asked to consent to their personal information relevant to a programme in which they may be enrolled in (in this case – Best Start Kōwae) to be sent to the PHO or the external health agency managing the programme (see Appendix A. PSAAP Enrolment Toolkit for PHO’s).
- If a patient is concerned about how their personal information is managed by the Gen2040 project, a privacy statement will be available via the Generation 2040 website. This privacy statement will describe how we access, use, store and retain personal information as part of the Gen2040 project. Providers will be instructed to refer the patient to the Gen2040
website regarding any privacy concerns. Providers will also be provided with the Gen2040 privacy statement when signing up to use the Best Start Kōwae.

4.3.2. Assessment of compliance

There will be no consequences should a patient decline to have the Best Start Kōwae. Patients are asked to provide written consent for instances like Best Start Kōwae when they enrol with their General Practice. A privacy statement regarding use of personal information in the Gen2040 project will be accessible via the National Hauora Coalition website.

4.3.3. Risk Assessment

The risk of this principle being breached is Medium. Even though consent is gained for instances like the Gen2040 project as part of the enrolment process with their general practice, patients may not feel comfortable completing the Best Start Kōwae. We have therefore implemented the following risk mitigation actions:

- Patients may decline to have the Best Start Kōwae completed.
- We will produce a privacy statement, which will be available via the National Hauora Coalition website.
- Providers will also be provided with the Gen2040 privacy statement when signing up to use the Best Start Kōwae.
4.4. **Principle 4 – Manner of collection of personal information**

Privacy Act Principle 4 – Manner of collection of personal information

Be fair and not overly intrusive in how you collect the information

HIPC Rule 4 - Health information must not be collected by unlawful means or by means that are unfair or unreasonably intrusive in the circumstances.

4.4.1. **How information is collected**

Information will be collected during private consultations between patients and their primary care or maternity care providers, as part of their normal clinical care.

4.4.2. **Assessment of compliance**

The method of collecting information from patients is aligned with their normal clinical care. Therefore, the means of collecting information is lawful and not overly intrusive. We have addressed considerations regarding consent, right to decline use of the Best Start Kōwae and purpose of collecting information in other principles.

4.4.3. **Risk Assessment**

The risk of breaching this principle is low.
4.5. Principle 5 – Storage and security of personal information

Principle 5 – Storage and security of personal information

Take care of it once you’ve got it and protect it against loss, unauthorised access, use, modification or disclosure and other misuse.

HIPC Rule 5 - It’s impossible to stop all mistakes. But health agencies must ensure that there are reasonable safeguards in place to prevent loss, misuse or disclosure of health information.

4.5.1. How we manage storage and security

All parties involved in the development and use of the Best Start Kōwae must adhere to the Health Information Privacy Code (1994) and Privacy Act (1993). This will be reinforced via Service Agreements with developers and users of the Best Start Kōwae.

<table>
<thead>
<tr>
<th>Safeguarding provider access to personal information</th>
<th>Only suitably qualified primary maternity care practitioners will have access to use the Best Start Kōwae (i.e., General Practitioners, nurses, midwives).</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A valid PHO PMS license is required to access and use Best Start Kōwae PMS.</td>
</tr>
<tr>
<td></td>
<td>Application and vetting process is carried out prior to users accessing Best Start Kōwae Online. The Gen2040 team will manage the vetting process to determine the appropriateness of user access to Best Start Kōwae online platform (e.g., the user must hold a current midwifery registration in New Zealand).</td>
</tr>
<tr>
<td></td>
<td>Best Start Kōwae Online access is provided via secure login and password via the Gen2040 project team. 2factor authentication is implemented and passwords will comply with “strong password” rules.</td>
</tr>
<tr>
<td></td>
<td>Authorised users have access to read, write, modify and update their patients’ health information only.</td>
</tr>
<tr>
<td></td>
<td>All health professionals are required to sign confidentiality agreements with their employer, which is applicable to access and use of the Best Start Kōwae.</td>
</tr>
<tr>
<td></td>
<td>Gen2040 also have confidentiality clauses stated within service agreements with providers (see Appendix A. Provider Service Agreement).</td>
</tr>
<tr>
<td></td>
<td>Gen2040 will recommend that all users complete privacy training via <a href="https://elearning.privacy.org.nz/">https://elearning.privacy.org.nz/</a> prior to use of the Best Start Kōwae.</td>
</tr>
</tbody>
</table>
4.5.2. Assessment of compliance

We have implemented a range of measures to safeguard access and storage of personal information (described above). User access to Best Start PMS and Best Start Online will be restricted to authorised users and only accessible via secure login.

4.5.3. Risk Assessment

The risk of breaching this principle is low.
4.6. **Principle 6 – Access to personal information**

<table>
<thead>
<tr>
<th>Privacy Act Principle 6 – Access to personal information</th>
</tr>
</thead>
<tbody>
<tr>
<td>People can see their personal information if they want to</td>
</tr>
</tbody>
</table>

**HIPC Rule 6 - People usually have a right to ask for access to health information that identifies them.**

However, sometimes, health agencies can refuse to give access to information, for instance because giving the information would:

- endanger a person’s safety
- prevent detection and investigation of criminal offences
- involve an unwarranted breach of someone else’s privacy.

### 4.6.1. How we manage patients accessing their personal information

Patients can request a printout copy of their Best Start Kōwae results via their Health Provider.

### 4.6.2. Assessment of compliance

The design of the Best Start Kōwae allows Health Provider users to printout and give a hardcopy version of the assessment results to their patient.

### 4.6.3. Risk Assessment

The risk of breaching this principle is low.
4.7. Principle 7 – Access to personal information

Privacy Act Principle 7 – Correction of personal information
They can correct it if it’s wrong, or have a statement of correction attached

HIPC Rule 7 - People have a right to ask health agencies to correct health information about themselves, if they think it is wrong.
If the health agency does not want to correct the information, it does not usually have to. But people can ask the health agency to add their views about what the correct information is.

4.7.1. How we manage patients request to correct information
Patients can request a correction in person via their Health Provider. Providers have the ability to access and update information in the Best Start Kōwae at any time.

4.7.2. Assessment of compliance
Requests for the correction of personal information is handled via the patient’s Health Provider.

4.7.3. Risk Assessment
The risk of breaching this principle is low.
4.8. Principle 8 – Accuracy of personal information

Privacy Act Principle 8 – Accuracy etc. of personal information to be checked before use
Make sure personal information is correct, relevant and up to date before you use it

HIPC Rule 8 - Before it uses or discloses health information a health agency must take reasonable steps to check that information is accurate, complete, relevant, up to date and not misleading.

4.8.1. How we manage accuracy of personal information

It is the responsibility of the health provider user to check the accuracy of personal information at the time of the consultation with the patient. Health providers should do this as part of their normal clinical care. Any risk of mis-information between the patient and their Health Provider will be managed by the Health Provider and is outside the scope of this PIA.

The Best Start Kōwae system will have built-in some data validation measures to decrease the risk of human error while completing the forms (i.e., Fields within the form will only accept valid clinical responses).

Gen2040 will conduct data checks and audits will be conducted monthly as part of the payment process to providers. These data checks are conducted by the Gen2040 data analyst and financial analyst and will check for any data outliers in data or human error. Health providers will be notified and requested to amend or explain any errors picked up by the Gen2040 data analyst or financial analyst. We will also be extensively testing Procon systems for data rules and accuracy prior to the rollout of the Best Start Kōwae.

4.8.2. Assessment of compliance

Health Provider users are appropriately qualified to ensure data accuracy when inputting information. In any case, human error is a minor risk and will be managed between the Health Provider and the patient. The Gen2040 team will perform data accuracy checks on information provided for the Gen2040 project. Any identified errors can be corrected by the health provider directly, via the Best Start Kōwae.

4.8.3. Risk Assessment

The risk of breaching this rule is low or outside the scope of this PIA.
4.9. Principle 9 – Not to keep personal information for longer than necessary

Privacy Act Principle 9 – Not to keep personal information for longer than necessary
Get rid of it once you’re done with it

HIPC Rule 9 - A health agency that holds health information must not keep that information for longer than is necessary for the purposes for which the information may be lawfully used.

4.9.1. How long we will store personal information

Personal information collected will be stored in accordance with the Retention of Health Information Regulations (1996). Personal information collected by Best Start Kōwae will remained stored in Cloud Catalyst Servers. Personal information collected for the purpose of the Gen2040 project, will be stored on National Hauora Coalition servers.

4.9.2. Disposal of personal information

Upon the completion of the storage period and with approval from the funder (MoH), personal information will be disposed of securely using an external secure destruction contractor.

4.9.3. Assessment of compliance

Storage will be in accordance with the Retention of Health Information Regulations (1996). Personal information will be disposed of securely, using external secure destruction contractor.

4.9.4. Risk Assessment

Both Catalyst Cloud and the National Hauora Coalition conduct work within the health sector and are aware of the regulations that uphold the storage of personal information. Based on this, the risk of breaching this rule is low.
### 4.10. Principle 10 – Limits on use of personal information

<table>
<thead>
<tr>
<th>Privacy Act Principle 10 – Limits on use of personal information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use it for the purpose you collected it for, unless one of the exceptions applies</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>HIPC Rule 10 - Health agencies must use health information for the same purpose for which they collected that information.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Other uses are occasionally permitted (for example because this is necessary to enforce the law, or the use is directly related to the purpose for which the agency got the information).</td>
</tr>
</tbody>
</table>

#### 4.10.1. Use of personal information

There are two core purposes for the use of personal information. Firstly, the use of personal information to carry out the functionality of the Best Start Kōwae. Secondly, to fulfil the objectives of the Gen2040 project.

**4.10.1.1. Best Start Kōwae**

Personal information will be used to support core functionalities of the Best Start Kōwae, including:

- Functionality that allows multiple health providers to access and update personal information in consultation with their patients at different time points (i.e., as the pregnancy journey progresses); and
- To support built-in decision support functionalities.

**4.10.1.2. Gen2040 project**

Personal information will be used to fulfil objectives of the Gen2040 project, including:

- To meet required BCTI payment claim details (i.e., NHI, HPI, Provider Name, Assessment name, date assessment completed);
- To provide payment and performance reporting to PHO’s; and
- Identify and report all equity-related areas of interest to providers, PHO’s, funders, internal researchers and programme evaluators.

#### 4.10.2. Assessment of compliance

Use of personal information is outlined above. Any amendments the above statements regarding use of personal information, will need approval (in writing) from our funders. This PIA will also be updated and reviewed by the Office of the Privacy Commision prior to implementation. There is a minor risk that individual use personal information outside the scope mentioned above. All members of the Gen2040 project team have therefore completed privacy training and signed confidentiality agreements as part of employment at the National Hauora Coalition.

**Risk Assessment**

The risk of breaching this rule is low.
4.11. Principle 11 – Limits on disclosure of personal information

Privacy Act Principle 11 – Limits on disclosure of personal information

Only disclose it if you’ve got a good reason, unless one of the exceptions applies

HIPC Rule 11 - Health agencies can only disclose health information in limited circumstances. One example is where another law requires them to disclose the information. Also, a health agency can disclose information if it reasonably believes, for example, that

- disclosure is one of the purposes for which the agency got the information
- disclosure is necessary to uphold or enforce the law
- disclosure is necessary for court proceedings
- the person concerned authorised the disclosure
- the information is going to be used in a form that does not identify the person concerned.

4.11.1. Circumstances where we will disclose personal information

Disclosure of personal information will be done in accordance with the Health Information Privacy Code (1994), that is, we will not disclose health information unless the following circumstances apply:

- Patients authorise the disclosure of personal information (in writing); and
- Disclosure for the purposes of reporting, which will be anonymised prior to reporting.

4.11.2. Assessment of compliance

Disclosure of personal information will be done in accordance with the Health Information Privacy Code (1994).

4.11.3. Risk Assessment

The risk of breaching this rule is low.
4.12. Principle 12 – Unique identifiers

**Principle 12 – Unique identifiers**

Only assign unique identifiers where permitted

Some agencies give people a “unique identifier” instead of using their name. Examples are a driver’s licence number, a student ID number, or an IRD number. A health agency cannot use the unique identifier given to a person by another agency. People are not required to disclose their unique identifier unless this is one of the purposes for which the unique identifier was set up (or directly related to those purposes).

4.12.1. Unique identifier used

Within the Best Start Kōwae platform the primary identifier for patients is the National Health Index (NHI). The NHI is a unique identifier assigned to every person who uses health and disability support services in New Zealand. The NHI number is used to promote accurate information sharing and patient identification. NHI is widely used throughout the New Zealand health systems and the Best Start Kōwae is a health system. Neither Procon nor National Hauora Coalition specifically allocate NHI numbers to patients, as the assignment is already completed by other agencies. An example is that Procon will receive patient data from General Practice already identified by a NHI number that is verified by the Ministry of Health through the patient register enrolment process.

Procon will also implement measures to verify the integrity of the NHI number at all stages (including transit and storage) using the NHI Validation Routine provided by the Ministry of Health\(^2\).

Use of NHI numbers in the implementation of Best Start Kōwae ensures a widely understood and referenced ID across primary and maternity care providers.

The National Hauora Coalition will only have access to personal information identifiable by NHI. We will not receive any immediately identifiable personal information such as first or last name.

4.12.2. Assessment of compliance

The unique identifier for all purposes is National Health Identifier (NHI), a widely used identifier in the health system. The National Hauora Coalition will only have access to personal information identifiable by NHI. We will not receive any immediately identifiable personal information such as first or last name.

4.12.3. Risk Assessment

The risk of breaching this rule is low.

---

5. Risk Management

5.1. Privacy Breach Scenarios

Table 2. shows some scenarios identified as having a possibility to occur during implementation of the Gen2040 project. Risk mitigation activities are addressed in Section 4.

<table>
<thead>
<tr>
<th>Risk Description</th>
<th>Persons affected</th>
<th>Likelihood of occurring</th>
<th>Impact, if realised</th>
</tr>
</thead>
<tbody>
<tr>
<td>Un-authorised user gains user credentials to access Best Start PMS or Best Start Online.</td>
<td>Patients, Health Provider</td>
<td>Very low – The un-authorised user would need access to the health provider’s login details. We mitigate this risk by implementing 2F authentication for Best Start online. The PMS version is outside the scope of this PIA and would need to be managed by the Provider.</td>
<td>High – PMS version: un-authorised user would have access to patient files saved on PMS. Online version: un-authorised user would have access to Best Start Online information (only after submitting NHI)</td>
</tr>
<tr>
<td>Personal information intended accidentally sent to external persons</td>
<td>Patients, health providers.</td>
<td>Very low – All datasheets will only be accessible via secure API. A login and password will be assigned to delegated internal Gen2040 team members only.</td>
<td>High – Would give unauthorised access to de-identified personal information.</td>
</tr>
<tr>
<td>Servers hacked</td>
<td>Patients</td>
<td>Low</td>
<td>High – Would give unauthorised access to de-identified personal information.</td>
</tr>
</tbody>
</table>
5.2. Risk Management Strategy

Table 2. details the risks identified during the PIA process and actions to mitigate and manage the risk. Please note that it is not the intention of this document to identify and eliminate every possible privacy risk, but to identify genuine risks that are not unreasonable or remote and provide appropriate pathways to addressing and eliminating/reducing risk.

Table 2. Risk Management Strategy

<table>
<thead>
<tr>
<th>Risk</th>
<th>Likelihood</th>
<th>Impact</th>
<th>Risk Management Approach</th>
<th>Warning Signs</th>
<th>Strategy in event of occurrence</th>
<th>Assigned to &amp; Escalation Pathways</th>
</tr>
</thead>
<tbody>
<tr>
<td>#R001 - Privacy breach in Procon or NHC servers</td>
<td>Low</td>
<td>High – compromises patient information</td>
<td>1. Physical Security: System housed in a secure data facility 2. Data storage and transfer: 2.1. Undertaken according to best practice standards 3. 128bit SSL / HTTPS encryption 4. De-identify all data on servers 5. Password protect access to servers 6. Conduct security audits prior to roll out (Internal and External)</td>
<td>Server logs application / web logs</td>
<td>1. Notify stakeholders in the “assigned to” 2. Immediately remove servers from the production environment &amp; remove user access 3. Follow best practice procedures for responding to a privacy breach 4. Notify relevant stakeholders of the breach – see “escalation pathways” 5. Conduct security audit (external)</td>
<td>Assigned to:  • Procon-hosted Server (Ken Leech/Procon Lead)  • Mōhio Server (Mōhio Team Lead/Generation 2040 Project Lead) Escalation Pathways: 1. Assigned to personnel to conduct necessary actions to resolve the breach. 2. Generation 2040 Project Lead to notify the Project</td>
</tr>
</tbody>
</table>
6. Report to appropriate stakeholders

Sponsor via incident report

3. Sponsor to notify the funder and request appropriate advice on notifying stakeholders.

4. Sponsor to initiate security audit of the relevant system where breach occurred.

5. Sponsor to report findings to funder.

6. Upon funder satisfaction, reinstate Best Start use.

#R002 - Cannot meet security / privacy requirements

<table>
<thead>
<tr>
<th>#R002 - Cannot meet security / privacy requirements</th>
<th>Low</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Undertake privacy impact assessment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Ensure full security audit prior to roll-out</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Ensure full understanding of responsibilities and notify the funder of any areas of concern immediately</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unable to identify security concerns, privacy queries etc via server / application / database logs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Conduct new privacy impact assessment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Conduct full security audit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Ensure full understanding of responsibilities and notify the funder of any areas of concern immediately</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Assigned to:
- Procon-hosted Server (Ken Leech/Procon Lead)
- Mōhio Server (Mōhio Team Lead)
- Generation 2040 Project Lead

Escalation Pathways:
7. Assigned to personnel to conduct necessary actions to address any concerns
<table>
<thead>
<tr>
<th>#R003 - Security updates to underlying software cannot be made</th>
<th>Low</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Ensure that system meets requirements of full security audit</td>
<td>Failure to patch successfully</td>
<td></td>
</tr>
<tr>
<td>1. Revert to previous version in production environment</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Raised by the funder.**

8. Generation 2040 Project Lead to notify the Project Sponsor via incident report.

9. Sponsor to notify the funder and request appropriate advice on notifying stakeholders.

10. Sponsor to initiate security audit and engage with funder on resolution.

**Assigned to:**
- Procon-hosted Server (Ken Leech/Procon Lead)
- Mōhio Server (Mōhio Team Lead/Escalation Pathways:

This risk should be managed by those in the “Assigned to” categories. The Generation 2040 project team will determine if a further escalation pathway is required.
5.3. Unanticipated Risk Management Strategy

Unanticipated risks may arise over the project lifecycle. Figure 2 displays management processes for managing unanticipated risks that may arise.

**Figure 2. Unanticipated Risk Management Flow**

- **Gen2040 Project Managers briefed on Risk**
- **Project Managers undertake Risk Assessment**
- **Risk deemed HIGH (i.e., major breach of security measures)**
  - Determine risk response within 24 hours of notification
  - Requires approval from Project Governance Group?
    - **Yes**: Project Governance Approval
    - **No**: Monitor risk response
  - Implement risk response
- **Risk deemed LOW (i.e., requires action, however does not impact service delivery)**
  - Notify key stakeholders
  - Add to risk register
  - Implement risk approach
  - Notify Governance Group
5.4. **Privacy Breach Response Plan**

### Notification of breach

- NHC data analyst identifies source of breach (i.e., NHC breach or Procon breach)
- Data analyst notifies Gen2040 Project Lead
- Gen2040 Project Lead notifies Gen2040 Data Governance Group and Project Sponsor
- Gen2040 Project Lead notifies Ministry of Health
- Gen2040 Project Lead notifies Office of Privacy Commissioner

### Breach response

- NHC/Procon Immediately remove servers from the production environment & remove user access
- Depending on nature of the breach, breach investigated and full report (including data compromised) produced by NHC/Procon.
- Breach fixes conducted by IT team where breach occurred.
- Project sponsor to contract external security organisation to perform audit on fixes

### Reinstating Best Start

- Once external audit completed and breach fixes are satisfactory, project Lead provides results to Office of Privacy Commissioner and Ministry of Health
- Best start reinstated upon approval (in writing) from Office of Privacy Commissioner and Ministry of Health.

6. **Conclusion**

This Privacy Impact Assessment (PIA) is for the Best Start Kōwae national roll out within Primary and Maternity Care, in conjunction with the Gen2040 project. This PIA includes considerations regarding the access, use, storage and security of personal information collected from patient’s (pregnant women engaging with their General Practice Providers or Midwives). All relevant considerations have been made and we are confident in our measures to mitigate any privacy risks to patients.
## Appendix A. Supporting Documents

<table>
<thead>
<tr>
<th>Best Start Cloud Risk Assessment</th>
<th>GEN2040_Cloud Risk Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provider Service Agreements</td>
<td></td>
</tr>
<tr>
<td>Privacy Statement</td>
<td></td>
</tr>
<tr>
<td>Penetration Testing Results</td>
<td></td>
</tr>
</tbody>
</table>