Patient experience surveys:

Privacy impact assessment report

Published August 2020

© Health Quality & Safety Commission New Zealand

Available online at www.hqsc.govt.nz

Enquiries to: info@hqsc.govt.nz

New Zealand Government

Contents

Abbreviations

Abbreviation	Meaning
Commission	Health Quality & Safety Commission
DCP	data collection portal
DHB	district health board
Governance Group	Patient Experience of Care Governance Group
HDEC	Health and Disability Ethics Committee
HIPC	Health Information Privacy Code 1994
HPI	Health Provider Index
IPES	inpatient experience survey
IPPs	information privacy principles
Ministry	Ministry of Health
NES	National Enrolment Service
NHI	National Health Index
NZISM	New Zealand Information Security Manual
PES	patient experience survey
PCPES	primary care patient experience survey
PHO	primary health organisation
PIA	privacy impact assessment
PMS	patient management system
SFTP	secure file transfer protocol
SMS	short message service (text)

1 Project summary

1.1 Background

The Health Quality & Safety Commission (the Commission) was set up under section 59 of the New Zealand Public Health and Disability Act 2000, 'to lead and coordinate work across the health and disability sector for the purposes of monitoring and improving the quality and safety of health and disability support services'. The relevant provisions in this legislation are set out in Appendix 1.

Since our establishment in 2010, we have designed and led improvement programmes across the health sector, with the aim of reducing harm and improving quality. Examples include programmes to reduce hospital-acquired infections, reduce falls and improve the safe use of medicines. We use information to monitor the processes and outcomes of these programmes and other important indicators of health system quality.

The Commission undertakes national patient experience surveys with the aim of improving the quality of health services in New Zealand by enabling patients to provide feedback that can be used to monitor and improve the quality and safety of health services. The surveys provide consistent tools that can be used for national measures as well as local assessment and improvement. Data is used by general practices, primary health organisations (PHOs) and district health boards (DHBs), as well as nationally across government.

Understanding the patient experience is vital to improving patient safety and the quality of service delivery. Growing evidence tells us that patient experience is a good indicator of the quality of health services. Better patient experience, stronger partnerships with consumers, and patient- and family-centred care have been linked to improved health, clinical, financial, service and satisfaction outcomes.

1.2 Patient experience surveys

The Commission's patient experience survey programme currently consists of two surveys: the inpatient experience survey (IPES), which began in August 2014, and the primary care patient experience survey (PCPES), which began in February 2016. Both now run quarterly nationwide. The surveys collect quantitative and qualitative data covering four key domains of patient experience: communication, partnership, coordination, and physical and emotional needs. To date, the IPES data set contains data from approximately 50,000 respondents, and the PCPES data set contains data from approximately 150,000 respondents.

The surveys are electronic, with invitations primarily sent by email or SMS. The IPES includes a mail-based option and the PCPES includes an option to be completed on a tablet. The IPES also allows DHBs the option of running the survey fortnightly to increase response numbers and support continuous quality improvement.

Patient feedback is anonymous and voluntary. Patients can choose to opt out of the survey.

Who will be surveyed?

The inpatient adult survey samples patients aged 15 years and older who have had at least one night's overnight stay, where the hospital event ended with a routine discharge or self-discharge. Specific exclusions are patients admitted to a mental health specialty, patients who were transferred to another health facility and patients who died in hospital.

The primary care survey samples enrolled patients aged 15 years and older who have had a consultation with the primary care service provider they're enrolled with during the survey sample period.

How will patients be surveyed?

Survey invitations will be emailed or texted to patients. Patients will receive a website link and be asked to complete the survey within 21 days.

Text messaging is provided as an option for Māori and Pacific populations to improve response rates from this group (up to a maximum of 5,500 texts per survey per quarter). Due to the cost of sending more than 5,500 texts each quarter, it is not possible to provide text messaging to everyone nationally.

How often will patients be surveyed?

The survey is conducted nationally every three months. Patients won't be asked to participate more than once every six months.

The sector (general practices, PHOs, DHBs and national users) access results through a secure online dashboard. There are limitations as to what results each organisation type can access (see the data access matrices in Table 2 and Table 3). There are currently approximately 1,500 sector users, with this number likely to grow. Data extracts are also provided to PHOs, DHBs and the Commission each quarter, with further extracts provided on agreement.

1.3 Key reference documents

- Adult hospital patient experience survey methodology and procedures 2020
- Primary care patient experience survey methodology and procedures 2020
- Patient experience survey questionnaire refresh. Summary of recommendations and revisions for inpatient and primary care surveys
- Adult hospital questionnaire 2020
- Primary care questionnaire 2020

1.4 Patient Experience of Care Governance Group

The successful performance of the national survey and reporting system is dependent on adequate and appropriate oversight, relationship management and review of the services performed.

The Patient Experience of Care Governance Group (the Governance Group) was established to provide independent advice to the Ministry of Health (the Ministry) and the Commission on the ongoing management of the adult inpatient and the primary care

patient experience surveys. This includes ensuring the results of the surveys are best used to improve the patient experience at local and national levels. The Governance Group is also providing governance on the collection, storage, access and use of the survey data until a broader information governance group is established.

Role

The role of the Governance Group is to:

- advise on the ongoing management of the two surveys
- advise on improving the survey tool and uptake of the surveys, in particular for Māori and high-priority populations
- champion the two surveys within the broader health sector and other stakeholders
- provide guidance that will enable the shift of focus from implementation of the survey to the use of the survey results to improve the health care experience of patients and communities
- support and advise on national publication of the survey results
- support and advise on increasing the profile of the surveys in the health sector and in communities
- ensure there is Māori participation and partnership in the ongoing management of the two surveys through appropriate clinical and consumer representation
- ensure that Māori data governance provisions are considered in collection, storage, use and sharing of survey data collected to align with the Te Mana Raraunga principles
- be fair, impartial, responsible and trustworthy.

Perspectives

The Governance Group will include perspectives of:

- Māori equity
- equity for Pacific and other high-priority populations
- PHOs and general practices
- DHBs and hospitals
- community and allied health
- consumers
- the Ministry of Health
- the Commission.

1.5 Need for this privacy impact assessment

The need for this privacy impact assessment (PIA) has arisen because the Commission undertook a competitive procurement process in 2019 for the national patient experience survey data collection and reporting system. This resulted in the selection of a new service and system provider, Ipsos Limited.

This PIA relates to the delivery of the national adult inpatient and primary care patient experience surveys from 2020, and any changes (if any) to the personal information involved and to how the information flows.

We are undertaking this PIA to discuss how we collect and report data from patients, DHBs, PHOs and the Ministry of Health from the early developmental stages of this new system through to when the system is adopted. This will be an evolving report. We want to ensure we have determined the best and safest approach to data transfer, storage and use. This will ensure we meet our legal and ethical responsibilities for data privacy, alongside our legislative objective to monitor health and disability services and our strategic priorities to improve consumer experience and health equity.

We also want to be able to give patients, DHBs, PHOs and the Ministry of Health confidence in our systems and processes, so they are comfortable with providing the required data. We take privacy seriously.

1.6 New data collection and reporting system from 2020

Ipsos will work with the key stakeholders to ensure the changeover from the existing services to the new services is a positive experience for the sector and meets current requirements.

The wider project also includes reviewing both the inpatient and primary care questionnaires, sampling methods, privacy impact assessment, cloud risk assessment, and ongoing communication and engagement with the stakeholders. Changes to the wider environment since 2014 mean that the data security and sovereignty requirements are of a higher standard than previously.

1.7 Review

This is a living document. Future review would be triggered by either a change in provider or a change to requirements.

Version control

Version	Date	Author	Rationale
1.1	July 2020	C Gerard	Updated to reflect processes with new survey provider and approved cloud risk assessment
1.2	Aug 2020	C Gerard	Update to show change in data flows for the primary care survey

2 Scope of the privacy impact assessment

This PIA has been undertaken in relation to the update of the data collection and reporting system for the adult inpatient and primary care patient experience surveys. The system provides national functionality to collect and report patient experience of health care for quality improvement purposes, with a focus on addressing inequities. The information collected contributes to the patient experience of care system level measure for primary care and DHBs, and the Commission's legislative objective and functions of monitoring the equity, quality and safety of health care (see Appendix 1).

We have designed the scope of this PIA to 'future-proof' ourselves for the addition of new surveys to the system, such as a mental health and addiction survey. That noted, we

realise that the scope and design of new programmes may vary from our current models, so there is a caveat that any new survey may need a full PIA.

2.1 In-scope questions

In terms of the Office of the Privacy Commissioner's information for agencies (Figure 1), our in-scope questions are as follows.

- Purpose:
  - To enable patients to provide feedback that can be used to monitor and improve the quality and safety of health services, what non-clinical and demographic consumer-level information do we need to collect from health care providers to send the surveys and then report the consumer feedback to health care providers in an actionable format?
- Agency responsibility:
  - How will information be transferred to the service provider, Ipsos?
  - How will information be stored by the service provider, Ipsos?
  - How will information be made available to health care providers?
  - How will we keep this information secure both in transit and at rest?
- Fair collection:
  - Is consumer consent required for collecting that data?
  - Who will collect the information?
  - How will we ensure the accuracy of the information?
- Justified use:
  - How will we use this information: de-identification, aggregation, analysis, presentation and publication?
  - Who will be able to access this information?
  - Will a third party be able to use information?
- Appropriate disposal:
  - How will we dispose of the information?

Figure 1: The Office of the Privacy Commissioner's conceptual diagram of information for agencies

Source: www.privacy.org.nz

2.2 In-scope and out-of-scope data use

Some aspects of data use by the Commission are out of scope for this PIA. These include:

- all data collected by the Commission for other quality improvement programmes or Quality and Safety Markers
- data collection from contracted providers or those without a direct health care role, including:
  - the Surgical Site Infection National Monitor, because this is a surveillance data set from different sources
  - hand hygiene data, which is collected through Hand Hygiene NZ
- data and information collected under mortality review committee legislation
- data collected by DHBs and other agencies for the Adverse Events Learning Programme.

Only data collected for the national patient experience surveys is in scope for this PIA.

2.3 The process

This PIA was undertaken by staff members from the Commission's Health Quality Intelligence team, with input from Corporate Services, DHBs and PHOs. We used the Office of the Privacy Commissioner's PIA template,[1] the Health Information Privacy Code 1994 (updated in September 2017)[2] and the Ministry of Health's Health Information Governance Guidelines[3] as primary references.

[1] www.privacy.org.nz/news-and-publications/guidance-resources/privacy-impact-assessment
[2] www.privacy.org.nz/assets/Files/Codes-of-Practice-materials/Consolidated-HIPC-current-as-of-28-Sept-17.pdf
[3] Ministry of Health. 2017. *Health Information Governance Guidelines*. Wellington: Ministry of Health.

The survey questionnaires and this PIA were submitted to the Health and Disability Ethics Committee (HDEC) for review. The HDEC concluded that the surveys are not within scope for it to review. For an observational study, HDEC must review it only if the study involves more than minimal risk (that is, potential participants could reasonably be expected to regard the probability and magnitude of possible harms resulting from their participation in the study to be greater than those encountered in those aspects of their everyday life that relate to the study).

The PIA process included:

- preparing a draft for internal team feedback
- having an independent review (by the Office of the Privacy Commissioner)
- preparing a revised draft for external feedback
- submitting the draft for HDEC review
- incorporating all feedback and, where necessary, making personal information flows or system changes to mitigate privacy risks
- gaining approval for and publishing the final report.

This PIA sits alongside a cloud risk assessment undertaken prior to contracting Ipsos and completing the PIA. The cloud risk assessment is designed to provide assurance that cloud service risks are managed. Given Ipsos's cloud service will contain information considered 'unclassified, in-confidence and sensitive', the service has been reviewed by our internal team and independent experts from Aura Information Security. Any risks identified are incorporated in the project planning and service provider agreement to ensure that the service, including all third-party contractors, meet our privacy and security requirements prior to the system going live. Any issues identified will be remedied, as agreed with the Commission, with appropriate timing relative to the risk.

Data breaches. The national head agreement requires Ipsos to manage and resolve any data breach in accordance with the Office of the Privacy Commissioner's privacy breach guidelines.[4] This includes immediate notification, communication and implementation of a solution.

We recognise that the Health Information Privacy Code 1994 (HIPC) applies to the work of the Commission. Section 4(1)(e) of the HIPC identifies that the HIPC applies to:

> (e) information about that individual which is collected before or in the course of, and incidental to, the provision of any health service or disability service to that individual.

Section 4(2)(k) specifies that the agencies it applies to include:

> (k) an agency which provides services in respect of health information, including an agency which provides those services under an agreement with another agency[5]

The HIPC gives specific guidance as to how we should undertake our PIA and understand and mitigate any privacy risks.

[4] www.privacy.org.nz/privacy-for-agencies/privacy-breaches
[5] www.privacy.org.nz/assets/Files/Codes-of-Practice-materials/Consolidated-HIPC-current-as-of-28-Sept-17.pdf

3 Personal information

This section shows the flow of information from collection at DHBs or primary care, through to the Commission, and our current plan to manage, handle and protect it.

The Privacy Act 1993 states personal information means information about an identifiable individual. Survey responses are not considered personal information unless they are linked to identifiable individuals, which most are not.

3.1 Purpose of information collection

Ipsos Limited has been contracted to provide the national data collection and reporting system in accordance with our methodology and procedures documents. A key requirement of the system is to seek and report patient feedback through electronic means enabling automated updates to online reports. The system is only accessed by authorised users and the information visible to users is in accordance with the data access matrices in Table 2 and Table 3.

This approach minimises administration for general practice, PHOs and DHBs, leads to higher-quality, more timely data through minimal intervention and allows for prompt report updates. Patients requesting contact can be triaged and attended to as soon as possible by an authorised system administrator in each organisation.

The inpatient survey rules also accommodate mailed surveys. This is to improve sample size and/or survey response rate.

A key requirement of the system is the provision of each patient's email address and mobile phone number.

Patient feedback is anonymous and voluntary. Patients can choose to opt out of the survey at multiple points.

3.2 Personal information involved

To collect data on patients' experience of care, we need to send people a unique survey link. Each survey sent has a unique ID that enables line-by-line analysis of responses, while the respondent remains anonymous.

When the patient data extract from DHBs or primary care (via the National Enrolment Service, NES) is imported to the national system, a number is assigned to each line of information. The national survey and reporting system doesn't require patient identifiable information to be held in the database. Initially personal information is needed to enable email and text correspondence to be addressed and sent but once each survey closes (three weeks after email and text surveys are sent), all identifiable information is deleted from the system. Note that each survey respondent's demographic information, such as age, gender and ethnicity, is retained.

All responses to the survey are anonymous unless respondents choose to provide their contact details because they wish to talk to someone at the DHB or their primary care provider.

Hospital patient data

Each DHB is responsible for extracting its patient data and importing it into the data collection portal for the quarterly survey. The patient extract should include all patients discharged in accordance with the patient data extract rules in the methodology and procedure document. The personal information securely transferred from the DHB's hospital system is as follows.

Field	Mandatory value	Example data
National Health Index (NHI) number	✓	CHB2702
Salutation	-	Mrs
First name	✓	Mary
Last name	✓	Smith
Address1	✓	1 Story Street
Address2	✓	Timaru
Address3	-	
Address4	-	
Post code	-	0931
Mobile phone	-	0279876543
Email address	-	marysmith@gmail.com
Gender	✓	F
Age	✓	38
Discharge date	✓	20110816 22:14:00
Ethnicity	✓	21
Health specialty code	✓	S00
Facility code	✓	D706
Admission type	✓	AC or AA or WN
DHB of domicile	✓	123 or 011
DHB of service	✓	123 or 011
Optional extra field x3		TBC

Primary care patient data

Patients aged 15 years and over who have received a consultation (as defined in the PHO services agreement) from the primary care service provider they are enrolled with during the survey sample week receive a survey invitation. Patient contact information to be used in the survey is captured within the Ministry's National Enrolment Service database. Practices can update the NES database in real time through their patient management system (PMS).

As most survey invitations are emailed to patients, invitation is reliant on practices collecting and accurately recording patient email addresses.

While it is best practice to collect individual email addresses for the primary care PES, the Office of the Privacy Commissioner has confirmed that shared email addresses (eg, familyinbox@gmail.co.nz) are acceptable. This is because the email invitation is personally

addressed so it is clear who is being invited to complete the survey. The wording of the email does not disclose recent attendance.

Shared mobile phone numbers (eg, with a spouse) are not used for survey invitations. This is because the text invitation is short and does not include a salutation, so it would not be clear who the invitation is for.

Due to a limited number of texts available, text invitations are sent only to Māori and Pacific peoples who don't have an email address. Further rules are applied during the extract to limit the number of SMS-only invitations sent by Ipsos to 5,500 per quarter. These rules stratify practices according the proportion of their enrolled population that is of Māori or Pacific ethnicity. Practices with a relatively high proportion of these groups in their population receive more of the SMS allocation than those with a lower proportion.

The personal information securely transferred by the Ministry of Health from the NES database is as follows.

Field	Data type	Mandatory value	Allowed options (if restricted)	Example data
NHI number	Alphanumeric	✓	-	CHB2702
Title I prefix	Text	✓	-	Mrs
First given name	Alphanumeric	✓	-	Jennifer
Family name	Alphanumeric	✓	-	Smith
Mobile phone	Alphanumeric		-	0279876543
Email address	Alphanumeric		-	david@gmail.com
Gender	Alphanumeric	✓	F M U O	F
Date of birth	Date	✓	-	19900615
Date of qualifying event	Date	✓	-	20110816
Ethnicity 1	Integer	✓	Only those codes in the Level 2 code table	21
Ethnicity 2	Integer	-	Only those codes in the Level 2 code table	
Ethnicity 3	Integer	-	Only those codes in the Level 2 code table	
HPI-O (practice)	Alphanumeric	✓		F2N084-H
HPI-O (PHO)	Alphanumeric	✓		F2N084-H
PHO Org ID	Alphanumeric	✓		794645
DHB of domicile (patient)	Integer	✓	DHB area codes	123 or 011
Practice DHB	Integer	✓	DHB area codes	123 or 011
Lead PHO DHB	Integer	✓	DHB area codes	123 or 011
Deprivation quintile	Integer	-	1 2 3 4 5	3
Community Services Card status	Text	-	Y N	Y

3.3 Informing patients of use of their information

Hospital

DHBs are aware of the need to inform patients of how the information they provide will be used. DHBs already have a statement in their registration/admission form that contains the following information:

> GENERAL PRIVACY STATEMENT
>
> We collect your health information to provide you with appropriate care, to plan for and fund health services, to carry out teaching and to monitor quality. We share this information with other health care providers and agencies involved in your care. We treat your information as confidential and ensure that it is kept secure and only accessed by authorised persons. You have a right to request access to your records and to request correction of the information. Information may be supplied to family, support people or other agencies if you give us your permission or disclosure is authorised by law.

This statement covers the collection of the patient's contact details to monitor quality through patient surveys.

Another useful statement we encourage DHBs to include would be worded along the following lines:

> PATIENT EMAIL ADDRESS FOR RECEIVING CLINICAL CORRESPONDENCE
>
> Please provide your email address if you are happy for <DHB> to send your clinical correspondence via e-mail. We may also invite you to give us feedback about your care. Please advise <DHB> as soon as possible in writing if your contact information changes.

This statement is useful given the patient's email address may be accessed by other people in the household. The email survey invitation includes an 'unsubscribe' option.

DHBs' public notices and 'your rights' brochures should also include similar information regarding the use of patient information for monitoring of quality. It would be useful to add collection of patient email addresses to these notices to increase the uptake and awareness of this among both patients and staff.

Primary care

PHOs and general practices are aware of the HIPC and the need to inform patients of the use of the information they provide. When patients enrol with a practice, they sign an enrolment form agreeing to the enrolment process and are informed about how their information will be used.

The patient enrolment form[6] (November 2018) contains the following to inform patients of the survey:

> **I understand** that the Practice participates in a national survey about people's health care experience and how their overall care is managed. Taking part is voluntary and all responses will be anonymous. I can decline the survey or opt out of the survey by informing the Practice. The survey provides important information that is used to improve health services.

Given this process will have occurred some time ago for many patients, the Commission needs people to be informed specifically about the survey. During the pilot phase, the Commission tested a range of ways to achieve this, although it is mindful no single method will ensure all patients are fully informed.

Participating PHOs and practices are provided with a range of resources by the Commission. These resources remind them of key dates and provide or link them to the following information:

- frontline staff guidance
- a display poster
- a survey slide that can be added to a TV slideshow if applicable for the practice
- a video that can be played during survey sample week
- a flyer to be handed out to all eligible patients during the survey sample week.

Practices can choose to text patients seen during the sample week to remind them they may receive a survey invitation. This action is optional for practices due to cost.

Practices are encouraged to use the Commission's resources during each survey period.

Practices are encouraged to ask for patients' email addresses during the sample week (individual rather than family addresses are preferred). Emailed survey invitations contain more information for the patients and may be more convenient.

Practices can record in their PMS patients who wish to opt permanently out of the survey.

The Office of the Privacy Commissioner has advised that this process is well inside the privacy rules: patients are notified and can say 'no'. All emails sent by the survey provider have a clear 'unsubscribe' option and if a patient clicks the unsubscribe button, no further emails will be sent to that email address.

[6] https://tas.health.nz/dhb-programmes-and-contracts/primary-care-integration-programme/primary-health-organisation-service-agreement-amendment-protocol/#Supporting

Figure 2: Information flow diagram – adult inpatient experience survey

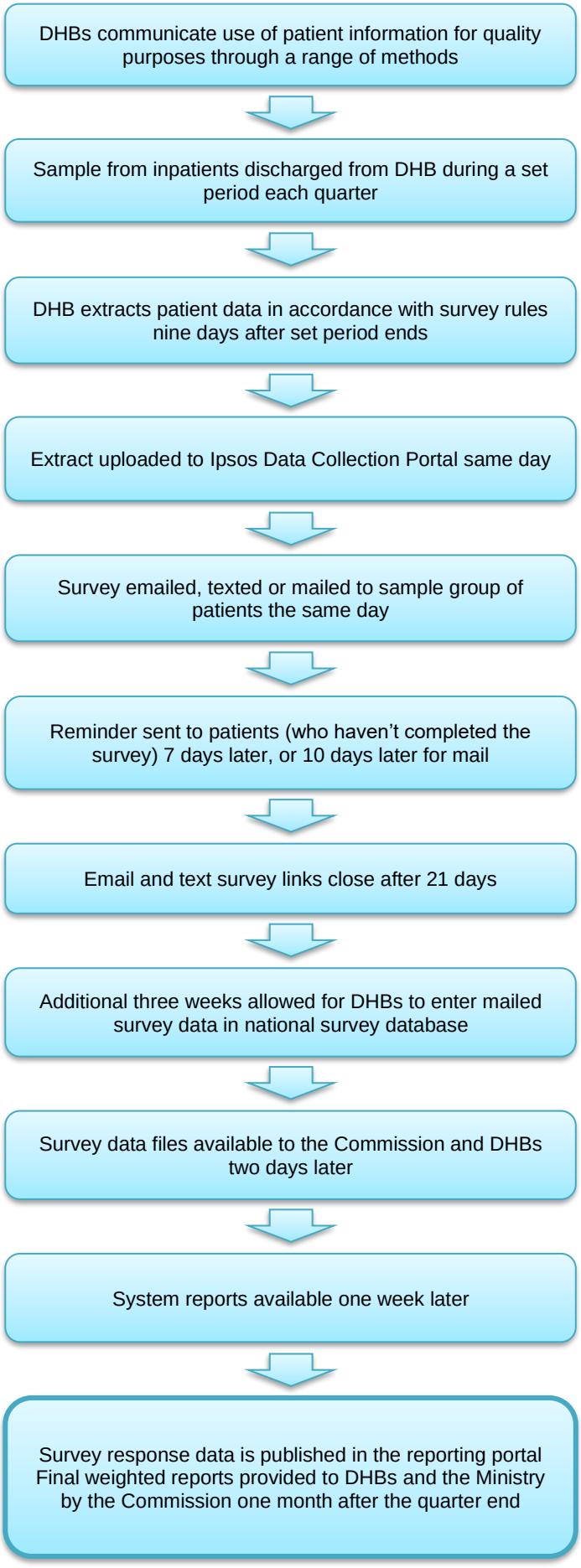

Figure 3: Information flow diagram – primary care patient experience survey

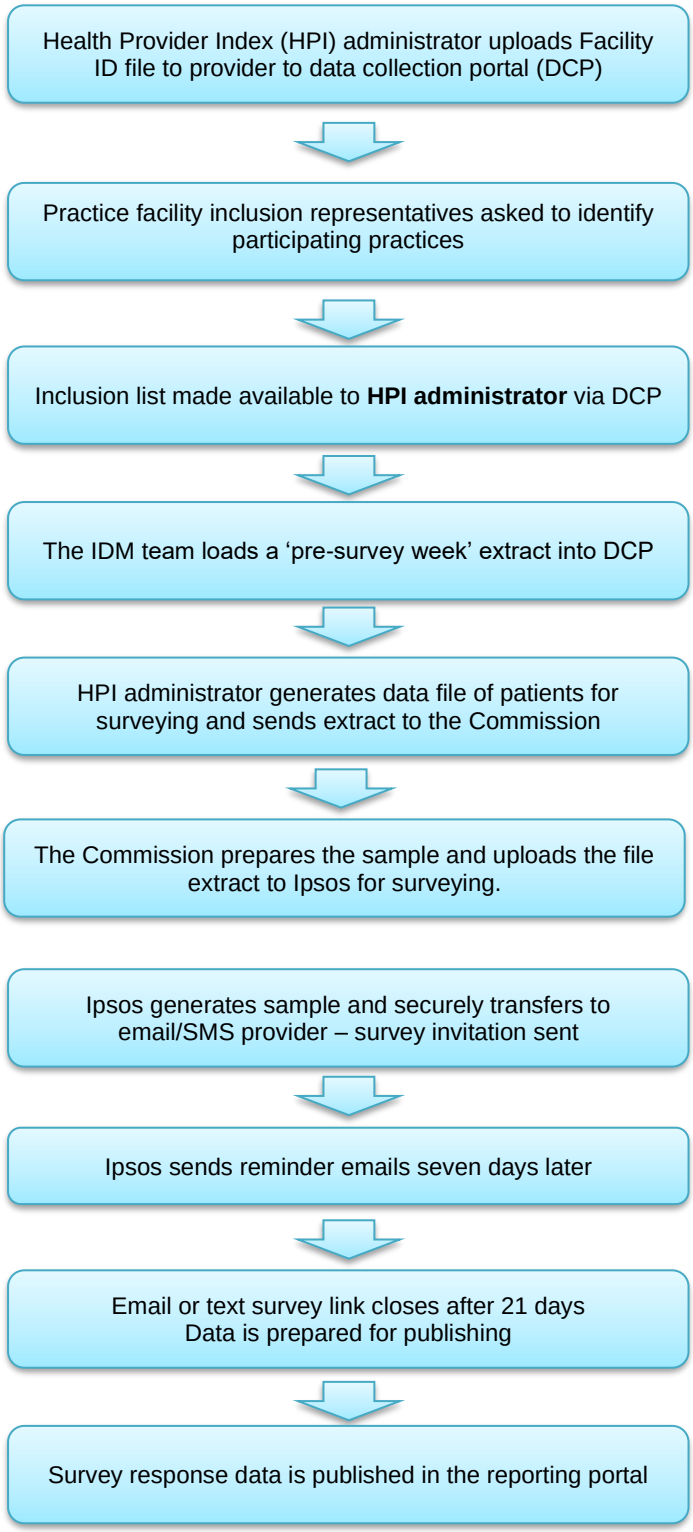

Table 1: Phases and timing of quarterly survey

Phase	Quarterly survey workflow – primary care survey	Timing	Example March–May 2020
Practice facility inclusion	Ipsos requests Facility ID file from **HPI administrator**	One month pre survey period	4 April (early reminder)
Practice facility inclusion	**HPI administrator** uploads Facility ID file to provider to DCP	One month pre survey period	6 April
Practice facility inclusion	Ipsos loads Facility ID file into Practice Facility Inclusion Interface	One month pre survey period	6 April
Practice facility inclusion	Practice facility inclusion representatives asked to identify participating practices	One month pre survey period	7 April
Practice facility inclusion	Deadline for PHOs to manage participating practices.	Two weeks pre survey period	23 April
Practice facility inclusion	Inclusion list made available to **HPI administrator** via DCP	Two weeks pre survey period	24 April
Pre-survey week testing phase	The IDM team runs a 'pre-survey period' extract against the inclusion list to check whether all practices can produce a list of eligible patients for the survey. Troubleshooting occurs in collaboration with the **Primary Care Programme Manager** and PHO champions. Fixes then improve the quality of the survey data file	Two weeks pre survey period	27 April – 4 May
Trial upload	The IDM team loads the 'dummy' extract into the DCP and Ipsos checks that the format and content are as expected. Ipsos and the IDM team work together to resolve any issues	During survey sample period (ideally only necessary for Wave 1)	4 May – 10 May 2020
Survey sample week	Survey sample period	As nominated by the Commission	4 May – 17 May 2020
Survey data collection	**HPI administrator** generates data file of patients for surveying and sends extract to the Commission. This is a record of all Qualified Encounter Dates received during survey period (including all contact details). **HPI administrator** sends version to the Commission with NHI numbers removed	Mon/Tues of week post survey period	11–12 May
Survey data collection	Commission prepares final extract and uploads to survey provider	Tues/Wed of week post survey period	12th and 13th May
Survey data collection	Ipsos emails or texts survey invitation to all patients in survey extract	Wed/Thur of week post survey	13–14 May

Survey data collection	Ipsos sends reminder emails seven days later	7 days after initial invitation	22 May
Survey data collection	Email or text survey link closes after 21 days	21 days after initial invitation	5 June
Follow-up	Follow up sector inquiries – Ipsos with input as required from the Commission and Ministry NES team and primary care teams	Ongoing	

3.4 Planned information flow changes

In the past, DHBs have had automatic uploads of data into the data collection portal. To begin with, this will be done manually by logging into the portal and uploading a file. This may be automated in future quarters.

3.5 Transfer and storage of information

The Commission has privacy and security requirements that must be met by Ipsos (and its contracted providers) in performance of its contracted services. These requirements endure beyond the expiry of the contract.

In the provision of its services, the supplier will comply with:

- HISO 10029:2015 Health Information Security Framework[7]
- the current version of the New Zealand Information Security Manual (NZISM) published by the Government Communications Security Bureau[8]
- the New Zealand Government Protective Security Requirements[9]
- the Privacy Act 1993, Health Information Privacy Code 1994 and other applicable legislation.

Ipsos must comply with any recommendations arising from this PIA as they relate to its services. The supplier will comply with any aspects of the 'patient experience survey data access guidelines' that apply to its services.

Ipsos must ensure that customer data is encrypted in storage and when in transit anywhere to or from the patient experience system, in accordance with NZISM. Any data is transferred using a secure file transfer protocol (SFTP).

Ipsos has an information security policy that is updated regularly and covers:

- computer acceptable use
- social media
- access policy
- mobile device use
- password policy
- physical security.

[7] www.health.govt.nz/publication/hiso-100292015-health-information-security-framework
[8] www.nzism.gcsb.govt.nz
[9] https://protectivesecurity.govt.nz/

Ipsos also has an information management policy that covers:

- information classification and labelling policy
- information handling policy
- information retention policy
- information destruction policy.

Ipsos Limited has contracted Lucidity Limited as its data hosting provider in New Zealand. Lucidity's IaaS services are delivered from Datacom NZ's Kapua data centre so that all data remains in New Zealand. Regular security and vulnerability testing is required.

The privacy and security requirements schedule and cloud risk assessment are available on request.

3.6 Access to information

The sector (general practices, PHOs, DHBs and national users) accesses survey results through a secure online reporting portal. All system users have unique logins, and database server access is separated and restricted to authorised staff.

The system's online reporting portal has been tailored to set appropriate user access rights. The data access matrices (Table 2 and Table 3) set out the levels of data access that have been agreed by the Patient Experience of Care Governance Group. Additional users, including those provided with a survey data extract for research purposes, will be assigned access rights that comply with the data access matrices.

3.7 Online reports

Within the portal it is possible to define the reports and administrative functions available to a user:

- in the report menu
- across the filters that are available
- in regard to administrative functions, for user management and moderation capabilities.

Users are able to download reports in formats such as PDF and images (png, jpg) for internal reporting.

Filtering

The reports are able to be filtered (using drop-down menus) for:

- date ranges
- age bands
- gender
- ethnicity
- practice DHB (DHB in which practice is located)
- lead PHO DHB (DHB that holds the PHO contract)
- DHB of domicile (DHB where the patient lives).

To prevent filters from allowing a patient to be identified, filtered results are automatically suppressed when fewer than five people meet the criteria. This protects patient privacy by

preventing analyses that show fewer than five responses, for instance, by a particular ethnicity in an age band with only a small number of respondents. This rule is an important way to prevent reports from becoming granular enough to breach patient anonymity.

3.8 Contact requests and free-text comments

Where patients have responded to the survey and requested contact from their practice or DHB, they provide their contact details as part of this request. If they choose, patients can request that the practice or DHB view their survey response. The key is that the individual decides what information can be viewed. The Commission does not see contact request information or any information that links an individual to their response.

Respondents can name individual providers in the free-text responses. Access to the free-text comments is controlled by a lead in each organisation and a protocol for reviewing has been developed (see Appendix 2).

Table 2: PCPES data access matrix – primary care

What can be seen									
Information	Data level	Patient	Practice	PHO	DHB	National	Commission	Approved research[a]	Public
Survey responses	Individual – identifiable	✓	✓[b]						
Online reporting portal – quantitative	Practice – their own, practice identifiable		✓	✓			✓		
	Practice – others in their PHO, practice anonymous		✓						
	All PHOs, PHO identifiable		✓	✓	✓[c]	✓	✓	✓	
	All DHBs, DHB identifiable		✓	✓	✓	✓	✓	✓	
Online reporting portal – qualitative comments	Individual (anon) – practice level, their own		✓	✓			✓		
	Individual (anon) – PHO level, their own			✓[d]			✓	✓	
	Individual (anon) – DHB level, their own				✓[d]		✓	✓	
Raw data extract	Unit record level (anon)			✓			✓	✓	
Published reports	High-level, national aggregate information	✓	✓	✓	✓	✓	✓	✓	✓

Notes:

[a] Approval granted by Governance Group, after a formal request and following the data access guidelines. If general practice-level identifiable data is sought, permission must be granted by PHOs in accordance with their individual practice data sharing protocols and agreements. Access to qualitative comments may be granted provided that comments can be cleaned to remove identifiable components.

[b] Only if patient requests contact and approves access to survey responses. Only accessed by nominated patient liaison.

[c] To be reviewed after six months.

[d] PHO super-user (person with administrative rights) sets permissions for those who can view comments.

Table 3: IPES data access matrix

What can be seen								
Information	Data level	Patient	PHO	DHB	National	Commission	Approved research[a]	Public
Patient data file (ex DHB)	Individual – identifiable			✓[b]				
Survey responses	Individual – identifiable	✓		✓[c]				
Online reporting portal - quantitative	All DHBs, DHB identifiable		✓	✓	✓	✓	✓	
Online reporting portal – qualitative comments	Individual (anon) – DHB level, their own		✓[d]	✓[d]		✓	✓	
Raw data extract	Unit record level (anon)			✓		✓	✓	
Published reports	High level, national aggregate information	✓	✓	✓	✓	✓	✓	✓

Notes:

[a] Approval granted by Governance Group, after a formal request and following the data access guidelines. Access to qualitative comments may be granted provided that comments can be cleaned to remove identifiable components.

[b] Only accessed by DHB administrator.

[c] Only if patient requests contact and approves access to survey responses. Only accessed by nominated patient liaison.

[d] DHB super-user (person with administrative rights) sets permissions for those who can view comments.

4 Privacy assessment

This section considers the privacy requirements that the Commission must follow to uphold the law, discusses possible risks related to the survey data collection and reporting system, and identifies our intended risk mitigation strategies.

The content is organised in Table 4 on the following pages, according to the 12 privacy principles of the Privacy Act 1993 and the corresponding rules of the HIPC.

Table 4: Assessment of compliance against privacy principles

#	Description of the privacy principle	Health Information Privacy Code (HIPC) rules	Summary of personal information involved, use and process to manage	Assessment of compliance	Risk analysis
1	Principle 1 – Purpose of the collection of personal information **Only collect personal information if you really need it.**	Rule 1 – Purpose of collection of health information Health information must not be collected by any health agency unless: (a) the information is collected for a lawful purpose connected with a function or activity of the health agency; and (b) the collection of the information is necessary for that purpose.	The information is required for PHOs, DHBs and the Commission to undertake the patient experience survey to monitor and improve the quality of their services. Without the information, we would be unable to seek and report patient feedback through an electronic, cloud-based means that ensures low cost and administration.	This process does not involve the collection of any information that is not required to complete the patient experience survey (PES). We consider that this proposal meets the requirements of this privacy principle and this HIPC rule.	The PES process collects only information that is required to complete the relevant PES and meet the PHO, DHB and Commission legislative requirements.
2	Principle 2 – Source of personal information **Get it directly from the people concerned wherever possible.**	Rule 2 – Source of health information (1) Where a health agency collects health information, the health agency must collect the information directly from the individual concerned. There are a range of exceptions allowed for agencies under the HIPC. Rule 2, exception 2(g) enables (g) that the information: (i) will not be used in a form in which the individual concerned is identified; (ii) will be used for statistical purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or (iii) will be used for research purposes (for which approval by an ethics committee, if	For the purposes of the PES, the non-clinical patient information required to send the survey and report the results is collected by: • the DHB directly from the patient and provided to Ipsos through an SFTP. DHBs, through their privacy statements and other notices, advise patients their contact information may be used to monitor quality • the practice directly from the patient and provided to the NES database. All practices' data (only that required for the survey) is then provided by NES to Ipsos through an SFTP. Practices, through their privacy statements and other notices, advise patients their contact information may be used to monitor quality. The information provided by the either the practice, NES or DHB will not be used in a form in which the	We consider that this proposal meets the requirements of this privacy principle and this HIPC rule.	We believe that our agency meets the exception stated in HIPC rule 2, 2(g) and consider the privacy risks associated with secondary collection for PES to be low.

		required, has been given) and will not be published in a form that could reasonably be expected to identify the individual concerned.	individual concerned is identified; will be used for statistical purposes and will not be published in a form that could reasonably be expected to identify the individual concerned.		
3	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.**	Rule 3 – Collection of health information from individual It is not necessary for an agency to comply with this rule, if it is not practicable for it to do so (rule 3, 4(c)).	Practices and DHBs collect the information directly from the patient for a range of purposes. The Commission, via Ipsos's system, collects patient feedback. The feedback is anonymous and voluntary. Patients can choose to opt out of the survey.	We consider that this proposal meets the requirements of this privacy principle and HIPC rule.	There is some risk, especially with primary care patients, that they may not be aware of the survey. We consider this risk to be low and have a range of notification options to mitigate it, including a patient 0800 helpline.
4	Principle 4 – Manner of collection of personal information **Be fair and not overly intrusive in how you collect the information.**	Rule 4 – Manner of collection of health information Health information must not be collected by a health agency: (a) by unlawful means; or (b) by means that, in the circumstances of the case: (i) are unfair; or (ii) intrude to an unreasonable extent upon the personal affairs of the individual concerned.	Practices and DHBs collect health information in a lawful manner with consideration of patients. At present, all practices and DHBs have processes in place for the collection of health information from both a clinical and a business perspective. The PES process will use information already collected more effectively. It does ask patients to complete a survey and this can be done in a timeframe to suit them. They will only receive one reminder and can choose to ignore it or opt out. None of the questions is compulsory to complete, so respondents may choose not to answer a question if they wish.	We consider that this proposal meets the requirements of this privacy principle and HIPC rule.	We consider that the manner of collection presents little risk with regard to the PES process.
5	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.**	Rule 5 – Storage and security of health information (1) A health agency that holds health information must ensure: (a) that the information is protected, by such security safeguards as it is reasonable in the	We have followed the Government's cloud computing requirements. The requirements are designed to provide assurance that cloud service risks are managed. The extent of assurance required depends on the sensitivity of the information the cloud service will contain. The PES information is	We consider that this proposal meets the requirements of this privacy principle and HIPC rule 5. Aura have completed an independent review of our cloud risk assessment.	There is always some risk where information is stored on cloud-based services. In the context of this PIA, this is possibly the higher-risk area, and there have been recent examples of unauthorised access to health data in other organisations. We have attempted to mitigate all possible risks within available

		circumstances to take, against: (i) loss; (ii) access, use, modification, or disclosure, except with the authority of the agency; and (iii) other misuse; (b) that if it is necessary for the information to be given to a person in connection with the provision of a service to the health agency, including any storing, processing, or destruction of the information, everything reasonably within the power of the health agency is done to prevent unauthorised use or unauthorised disclosure of the information; and (c) that, where a document containing health information is not to be kept, the document is disposed of in a manner that preserves the privacy of the individual. (2) This rule applies to health information obtained before or after the commencement of this code.	'unclassified, in-confidence and sensitive'. The Commission has privacy and security requirements that must be met by Ipsos (and its contracted providers) in performance of the services. These requirements endure beyond the expiry of the contract. In the provision of the services, the supplier will comply with: • HISO 10029:2015 Health Information Security Framework[10] • the current version of the New Zealand Information Security Manual published by the Government Communications Security Bureau[11] • the New Zealand Government Protective Security Requirements[12] • the Privacy Act 1993, Health Information Privacy Code 1994 and other applicable legislation. Ipsos must comply with any recommendations arising from this PIA as they relate to its services. The supplier will comply with any aspects of the 'patient experience survey data access guidelines' that apply to its services. Ipsos must ensure that customer data is encrypted in storage and when in transit anywhere to or from the patient experience system, in accordance with NZISM. Any data is transferred using an SFTP.		funding to follow best practice in this area.

[10] www.health.govt.nz/publication/hiso-100292015-health-information-security-framework
[11] www.nzism.gcsb.govt.nz
[12] https://protectivesecurity.govt.nz

			Ipsos has an information security policy that is updated regularly and covers: • computer acceptable use • social media • access policy • mobile device use • password policy • physical security. Ipsos also has an information management policy that covers: • information classification and labelling policy • information handling policy • information retention policy • information destruction policy. Ipsos Limited has contracted Lucidity Limited as its data hosting provider in New Zealand. Lucidity's IaaS services are delivered from Datacom NZ's Kapua data centre so that all data remains in New Zealand. Regular security and vulnerability testing is required. Safeguards include: physical security; IT security; staff training; policies that staff have to observe; and confidentiality clauses in contracts with external providers.		
6	Principle 6 – Access to personal information **Where an agency holds personal information in such a way that it can be readily retrieved, individuals should have access to their personal information.**	Rule 6 – Access to personal health information	This project involves the Commission holding identifiable patient contact information for a maximum of seven days each quarter. This is to allow the Commission to prepare the survey sample. This information cannot be linked to survey responses. Patient contact information is subject to these safeguards: physical security; IT security; limited staff access; staff training and policies; specific access data agreement.	We consider that this proposal meets the requirements of this privacy principle and HIPC rule 6.	We consider that there is little risk with regard to this process and principle. The agency will not hold readily identifiable personal information and cannot retrieve or provide access to it.

			The Commission does not hold survey response information in any form that would make it readily retrievable for any individual. As the Commission has no way of identifying individuals within the information provided to us by practices or DHBs, we will not be able to provide individuals with access, with one exception. Where patients have responded to the survey and requested contact from their practice or DHB, they provide their contact details as part of this request. If they choose, patients can request that the practice or DHB view their survey response. The key is that the individual decides what information can be viewed. The Commission does not see contact request information or any information that links an individual to their response. Respondents can name individual providers in the free-text responses. Access to the free-text comments is controlled by a lead in each organisation and a protocol for reviewing has been developed (see Appendix 2). At no stage will the Commission have survey response information that can easily identify individuals.		
7	Principle 7 – Correction of personal information **They can correct it if it's wrong, or have a statement of correction attached.**	Rule 7 – Correction of health information	At present, any request for the correction of a patient's health information would be recorded in the PMS. This request would generally come from the patient viewing their own health records either by face-to-face viewing of the electronic records or by sighting a printout of	The Commission will not be able to identify individuals in the data we hold, so cannot provide access nor the opportunity to correct. We consider that this proposal meets the requirements of this privacy principle and HIPC rule.	We consider that this proposal meets the requirements of this privacy principle and HIPC rule 7. The agency will not hold personally identifiable information and cannot correct it.

			the health information. This project has no impact on this. Health information should only be corrected at the source within practices or DHBs. The PES system has no functionality to correct patient records. It can unsubscribe a patient from the survey though.		
8	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.**	Rule 8 – Accuracy etc of health information to be checked before use (1) A health agency that holds health information must not use that information without taking such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date, complete, relevant and not misleading. (2) This rule applies to health information obtained before or after the commencement of this code.	DHBs, PHOs and practices are already subject to the Privacy Act 1993 regarding this principle and are required to ensure information is up to date and complete. This project has no impact on this process. The Commission requests the most up-to-date data from the practices and DHBs, to ensure that we get the most up-to-date and correct information. The survey is carefully timed to ensure this.	We consider that this proposal meets the requirements of this privacy principle and HIPC rule.	We consider that there is little risk with regard to this process and principle.
9	Principle 9 – Not to keep personal information for longer than necessary **Get rid of it once you're done with it.**	Rule 9 – Retention of health information (1) A health agency that holds health information must not keep that information for longer than is required for the purposes for which the information may lawfully be used. (2) Subrule (1) does not prohibit any agency from keeping any document that contains health information the retention of which is necessary or desirable for the purposes of providing	This project does not alter how DHBs or practices hold personal information, or the length of time for which they hold it. Any personal information collected to enable the surveys to be addressed and sent to patients is deleted once the survey has closed. Information will be destroyed in accordance with Ipsos's information destruction policy.	We consider that this proposal meets the requirements of this privacy principle and HIPC rule.	We consider that there is little risk with regard to this process and principle.

		health services or disability services to the individual concerned. (3) This rule applies to health information obtained before or after the commencement of this code.			
10	Principle 10 – Limits on use of personal information **Use it for the purpose you collected it for, unless one of the exceptions applies.**	Rule 10 – Limits on use of health information A health agency that holds health information obtained in connection with one purpose must not use the information for any other purpose unless the health agency believes on reasonable grounds: (e) that the information: (i) is used in a form in which the individual concerned is not identified; (ii) is used for statistical purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or (iii) is used for research purposes (for which approval by an ethics committee, if required, has been given) and will not be published in a form that could reasonably be expected to identify the individual concerned.	The purpose of the Commission having this information is for us to uphold our legislative responsibility to monitor the quality and safety of the health and disability sector. It will not be used for any other purpose than collecting feedback from patients on their health experience. Currently health information in practices, PHOs and DHBs is obtained in line with the information privacy principles (IPPs) and the set guidelines as to the use of that information. Generally, all health information is stored in the patient management system. When patients are admitted to hospital, they are advised of the use of the health information. All DHB staff and the privacy officer (or team) within the DHB are then the guardians of the information and are tasked with ensuring the information is used according to the IPPs. In primary care, patients are given a PHO enrolment form that outlines the use of the health information when enrolling with the practice. The practice team and privacy officer within the practice are then the guardians of the information and are tasked with ensuring the	We consider that this proposal meets the requirements of this privacy principle and HIPC rule. The requirements of the HIPC rule 10, exception 1(e) are met. This project will have no impact on this rule as DHBs already advise patients their information may be used to monitor quality. This project will have an impact on the use of primary care non-clinical information; however, patients are advised of this and that participation is voluntary and anonymous. They are also advised how to opt out of their information being used for this purpose.	We consider that this proposal meets the requirements of this privacy principle and HIPC rule. The requirements of the HIPC rule 10, exception 1(e) are met.

			information is used according to the IPPs.		
11	Principle 11 – Limits on disclosure of personal information **Only disclose it if you've got a good reason, unless one of the exceptions applies.**	Rule 11 – Limits on disclosure of health information (1) A health agency that holds health information must not disclose the information unless the agency believes, on reasonable grounds: (c) that the information: (i) is to be used in a form in which the individual concerned is not identified; (ii) is to be used for statistical purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or (iii) is to be used for research purposes (for which approval by an ethics committee, if required, has been given) and will not be published in a form that could reasonably be expected to identify the individual concerned;	The Commission does not intend to publish or disclose any individual-level information (including de-identified information). The information reported to practices, PHOs and DHBs will be reported in accordance with the data access matrices. Suppression techniques will also apply where there are small numbers for any group as additional risk management.	We consider that this proposal meets the requirements of this privacy principle and HIPC rule. The requirements of the HIPC rule 11, exception 2(c) are met.	We consider that there is little risk with regard the PES process proposed.
12	Principle 12 – Unique identifiers **Only assign unique identifiers where permitted.**	Rule 12 – Unique identifiers (1) A health agency must not assign a unique identifier to an individual unless the assignment of that identifier is necessary to enable the health agency to carry out any one or more of its functions efficiently.	This project will have an impact on this rule as the national survey and reporting system will assign a unique identifier to each survey sent, which is unrelated to the NHI number. This is to enable survey responses to be anonymous (unless the patient asks to be contacted by the practice or DHB and explicitly gives their permission for their	We consider that this proposal meets the requirements of this privacy principle, as unique identifiers are needed to record survey responses and monitor quality efficiently.	We consider that there is little risk with regard to the PES process proposed.

			survey response to be viewed by the practice or DHB) and incorporated in aggregated reports. Only the national system provider can link a patient's identifiable data to the unique identifier, and only for the period that identification data is retained in the system.		

5 Risk assessment

Based on our privacy assessment, we consider the risks from the patient experience data collection and reporting system to be low, with good mitigation strategies already in place and further mitigation to be completed before the new system is adopted.

The privacy assessment revealed that there are areas where the patient experience data collection and reporting system fits within allowable exceptions, or has some risks requiring mitigation. These exceptions and risks are summarised below.

5.1 Summary of exceptions and risks

- Source of personal information: We are not collecting data directly from individuals, but are using data from health records, provided by practices and DHBs (secondary collection).
- We are not directly disclosing or requesting permission from individuals for the use of their data; however, we do require both practices and DHBs to do so.
- We cannot provide opportunities for individuals to correct data.
- The national survey and reporting system will assign a unique identifier to each survey sent, which is unrelated to the NHI number.

Below, we provide further commentary about the issues we considered and our proposed actions to address them.

5.2 Source of personal information (principle 2, rule 2)

We are not collecting data directly from individuals, but are using data from health records, provided by practices and DHBs (secondary collection).

We are relying on secondary collection from practices and DHBs, which we believe is appropriate due to the following exclusions to principle 2.

- Getting the data from practices and DHBs will not prejudice the individual's interests.
- The information will not be used in any way that identifies the individual concerned.
- Collecting this information from practices and DHBs will protect public revenue and enable practice, PHO and DHB staff to spend less time collecting the data and providing it to the Commission.
- Collecting this information from the individuals concerned is not practicable.

The HIPC provides specific exceptions that the Commission's PES fits within. Rule 2, exception 2(g) enables

> (g) that the information:
>
> (i) will not be used in a form in which the individual concerned is identified;
>
> (ii) will be used for statistical purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(iii) will be used for research purposes (for which approval by an ethics committee, if required, has been given) and will not be published in a form that could reasonably be expected to identify the individual concerned.[13]

The Health Information Governance Guidelines 2017 outline policies, procedures and other useful details for health providers who collect and share personal health information, enabling them to implement these legally, securely, efficiently and effectively. These guidelines note:

> The use of health information for secondary purposes is permissible where the purpose was identified and stated at the point of collection, or where the information is used for research or statistical purposes but not published in a way that identifies the consumer.[14]

While appropriate for the purposes of patient experience monitoring, this method of collection has roll-on effects for other privacy principles and HIPC rules (3 and 7), which are discussed below.

5.3 Disclosure and permission seeking from individuals (principle 3, rule 3)

Because there is no direct engagement with individual consumers with regard to the collection of their personal information to send the PES, it is not practicable to disclose or seek permission. Practice and DHB staff will use medical records to provide patients' contact and demographic information for the purposes of the survey. This proposed secondary data use is more practical and cost-effective than gathering information directly from individuals, representing more appropriate use of limited health sector resources. We can also invite substantially more patients to give feedback on their health experience.

We consider that this proposal meets the requirements of the Health Information Governance Guidelines 2017[15] for secondary use of data, as highlighted in the quote above. The information collected through secondary processes will be used for statistical purposes with no identification of individuals. The Health Information Governance Guidelines 2017 support the secondary use of health information without requiring practice or DHB staff to check with the individuals concerned.

5.4 Storage and security of personal information (principle 5, rule 5)

Storage and security of personal information has been reviewed in a separate cloud risk assessment. The PES uses cloud-based services to transit and store data within New Zealand, which always involves some risks. In the context of this PIA, this is possibly the higher-risk area. Recent examples of unauthorised access to health data in other organisations highlight this risk.

---

[13] www.privacy.org.nz/assets/Files/Codes-of-Practice-materials/Consolidated-HIPC-current-as-of-28-Sept-17.pdf (page 9).
[14] www.health.govt.nz/our-work/ehealth/digital-health-sector-architecture-standards-and-governance/health-information-standards/approved-standards/hiso-100642017-health-information-governance-guidelines (page 28).
[15] www.health.govt.nz/our-work/ehealth/digital-health-sector-architecture-standards-and-governance/health-information-standards/approved-standards/hiso-100642017-health-information-governance-guidelines

We have followed the Government's cloud computing requirements. The requirements are designed to provide assurance that cloud service risks are managed. The extent of assurance required depends on the sensitivity of the information the cloud service will contain. The PES information is 'unclassified, in-confidence and sensitive'.

The Commission has privacy and security requirements that must be met by Ipsos (and its contracted providers) in performance of its services. These requirements endure beyond the expiry of the contract. In the provision of the services, the supplier will comply with:

- HISO 10029:2015 Health Information Security Framework[16]
- the current version of the New Zealand Information Security Manual published by the Government Communications Security Bureau[17]
- the New Zealand Government Protective Security Requirements[18]
- the Privacy Act 1993, Health Information Privacy Code 1994 and other applicable legislation.

Ipsos must comply with any recommendations arising from this PIA as they relate to Services. Ipsos must ensure that the data is encrypted in storage and when in transit anywhere to or from the patient experience system, in accordance with NZISM. Any data is transferred using an SFTP.

Safeguards include physical security; IT security; staff training; policies that staff must observe; and confidentiality clauses in contracts with external providers. We have attempted to mitigate all possible risks within available funding to follow best practice in this area.

5.5 Offering individuals the opportunity to correct data (principle 7, rule 7)

As the Commission will itself not be able to identify individuals in the data we hold, we cannot provide access, nor the opportunity to correct data records, to individuals.

However, the information the Commission will be relying on can be checked and corrected in the original record within practices and DHBs, where the information is collected and stored. Patients can request to view and/or correct their health information within practice or DHB records. This project has no impact on this.

5.6 Unique identifiers (principle 12, rule 12)

This project will have an impact on this rule as the national survey and reporting system will assign a unique identifier to each survey sent, which is unrelated to the NHI number. This is to enable survey responses to be anonymous (unless the patient asks to be contacted by the practice or DHB and explicitly gives their permission for their survey response to be viewed by the practice or DHB) and incorporated in aggregated reports.

Only the national system provider can link a patient's identifiable data to the unique identifier, and only for the period that identification data is retained in the system.

[16] www.health.govt.nz/publication/hiso-100292015-health-information-security-framework
[17] www.nzism.gcsb.govt.nz
[18] https://protectivesecurity.govt.nz/

6 Recommendations to minimise impact on privacy

As a result of this PIA, we make the following recommendations to address the Commission's processes and risk mitigation.

1. Collection of information: The Commission should provide national tools as a way of continuing to support and encourage practices and DHBs to notify patients of the collection of their information for survey purposes.
2. Storage and security: Ensure the Agreement's requirements under Schedule Three need to be maintained, including routine system testing.
3. Limits on disclosure of personal information: Ensure that part of the project testing stage is to report information to practices, PHOs and DHBs in accordance with the data access matrices and that suppression techniques are applied for small numbers when reports are 'drilled down'.

7 Action plan

We propose the following actions for the Commission as a result of this PIA.

Ref	Agreed action	Who is responsible	Completion date
A-001	Ipsos will provide an internal vulnerability scan and independent penetration and stress testing to ensure that the service, including all third-party contractors, will meet the Agreement's Schedule Three privacy and security requirements prior to the system going live, at their own cost. Any issues identified will be remedied, as agreed with the Commission, with appropriate timing relative to the risk rating, at Ipsos's own cost.	Ipsos	July 2020
	Independent review of the cloud risk assessment	Commission/Aura	7 February 2020
	Review this PIA and the cloud risk assessment once system testing is complete, before the system is adopted	Commission	August 2020
	Establish a contract operations group to: • review and monitor the working relationship of the partnership • review the progress and completion of services • prioritise and approve new services.	Commission/Ipsos	
	The data access matrices are maintained by the Commission and any changes approved by the Governance Group.	Commission	

Appendix 1: Provisions in the New Zealand Public Health and Disability Act 2000 related to objectives and functions of the Commission

59B Objectives of the Health Quality & Safety Commission (HQSC)

The objectives of HQSC are to lead and co-ordinate work across the health and disability sector for the purposes of—

(a) monitoring and improving the quality and safety of health and disability support services; and

(b) helping providers across the health and disability sector to improve the quality and safety of health and disability support services.

Section 59B: inserted, on 9 November 2010, by section 17 of the New Zealand Public Health and Disability Amendment Act 2010 (2010 No 118).

59C Functions of HQSC

(1) The functions of HQSC are—

(a) to advise the Minister on how quality and safety in health and disability support services may be improved; and

(b) to advise the Minister on any matter relating to—

(i) health epidemiology and quality assurance; or

(ii) mortality; and

(c) to determine quality and safety indicators (such as serious and sentinel events) for use in measuring the quality and safety of health and disability support services; and

(d) to provide public reports on the quality and safety of health and disability support services as measured against—

(i) the quality and safety indicators; and

(ii) any other information that HQSC considers relevant for the purpose of the report; and

(e) to promote and support better quality and safety in health and disability support services; and

(f) to disseminate information about the quality and safety of health and disability support services; and

(g) to perform any other function that—

(i) relates to the quality and safety of health and disability support services; and

(ii) HQSC is for the time being authorised to perform by the Minister by written notice to HQSC after consultation with it.

Appendix 2: Protocol for reviewing patient comments

Background

Understanding patients' experience is vital to improving patient safety and the quality of care. The Ministry of Health and the Health Quality & Safety Commission are introducing an online patient experience survey for primary care. Patient participation is voluntary and their responses will be anonymous unless they choose to provide their contact details.

The survey consists of different modules that patients complete according to which health services they have accessed in the last year. There is space for patients to provide one or more free-text comments in each of the modules; in total the survey contains 22 places where a comment can be made.

Viewing patient comments

All comments made by patients are anonymous for the patient; however, some comments can identify a practice, staff member or other health organisation.

Different organisations have different levels of access.

- Practices can only view comments made by their patients.
- In a PHO, the super-user (person with administrative rights) sets permissions for who is able to view comments. Comments are viewable for each of their enrolled practices by name.
- In a DHB, the super-user sets permissions for who is able to view comments. Comments are viewable at the PHO level, and only for PHOs where they are the lead DHB. The comments are not identifiable by practice.

Why comments need to be reviewed

There are important reasons why a systematic process and timely approach to reviewing patient comments is needed. These include:

- ensuring that 'hate speech' is identified and removed
- removing staff or practice identifiable comments where requested
- identifying and acting on serious issues such as safety, violence or a serious complaint
- identifying and acting on matters that require follow-up, for instance. a broken handrail in the clinic.

Who should review comments

This is a skilled task and comments should be reviewed by someone who is a quality manager or in a similar role. The reviewer looks for common threads and should be in a position to take appropriate action in response.

Common definitions

Text moderation: This is the process of editing patient comments. Original comments remain accessible to super-users in the text moderation area; that is, if they edit a comment, they see the original comment and the edited comment.

Super-user: This is the person who has administrative rights for their organisation on the patient experience survey dashboard.

Patient contact request. This is where a patient requests that their practice contact them to discuss their feedback or health experience. Currently, Cemplicity emails practices the contact requests.

Principles for reviewing comments

- In general, swear words do not need to be moderated as they are considered part of normal language.
- Comments that identify practices and staff do not need to be moderated before they appear on the reporting portal. However, identifiable comments can be moderated on request.
- Any editing of text should be minimal and as far as possible retain the strength and intent of the original comments.
- Practice leaders or managers should be made aware of the original comment when identifiable information is changed.
- Where comments about identifiable staff are positive, they should not be edited. The staff member can still request comment moderation.
- Where comments are negative and identify a staff member, editing should focus on the behaviour and experience rather than the staff member's specific role or personal description.
- Hate speech should always be edited.

Process for reviewing comments

The survey is sent out to patients 10 days after the end of the survey sample week. Patients have 21 days to respond to the survey, after which it closes and they can no longer complete it.

It is strongly recommended that all comments are reviewed within a month of the survey closing; however, it is considered good practice to review comments at least weekly during the three-week period that survey responses are completed. This will ensure that serious issues are identified in a timely manner.

The table below describes the process and recommended actions.

Comment that triggers action	Recommended action for super-user	Notify practice
a. Swearing or offensive comment	Hate speech is to be edited[19]. Use square brackets [ ] to indicate text has been removed or altered Swear words do not generally require editing	No
b. Comment identifies a practice, practitioner, reception staff or another patient	Do not edit these unless requested. Where comment are edited, the practice leader or manager should be made aware of the original comment Replace identifiable names with generic terms, eg, [nurse] [doctor] [A&M clinic]	Yes
c. Comment identifies patient, eg, name, phone number, home address.	Replace specific details that identify the patient or their clinical condition using [generic terms]. Clinical details such as condition, specific medication or history that are linked to a personally identifiable patient should be edited	No
d. Comment raises an issue of a serious nature, eg, safety, violence, suicide or serious complaint, and the patient is identifiable	PHO should use its serious complaints procedure	According to protocol
e. Comment identifies some other action. This might require something to be fixed, eg, broken handrail in the clinic or a medication error	PHO should email the practice to alert it	Yes

Privacy considerations

In the instructions for each section of the survey, patients are advised that any comments they write are anonymous, which means no one reading those comments will know who wrote them. Only some people (including those at their general practice) will read the comments to help them understand the service and how to improve it.

To respect the privacy of practices, practice staff and other health providers and professionals, it is important that login details to the primary care patient experience portal are shared judiciously.

The table below sets out who might be expected to view patient comments. Practices are encouraged to share their login widely within their general practice team, as these are their results. Logins within a PHO or DHB and at the national level should be restricted to only those whose role necessitates access. The table below suggests, by organisation, who might have access and what their level of access is.

[19] Hate speech is prohibited under the Human Rights Act 1993. Section 61 (Racial disharmony) makes it unlawful to publish or distribute 'threatening, abusive, or insulting … matter or words likely to excite hostility against or bring into contempt any group of persons … on the ground of the colour, race, or ethnic or national or ethnic origins of that group of persons'. Section 131 (Inciting racial disharmony) lists offences for which 'racial disharmony' creates liability.

Organisation	Role	View
Practice	General manager, practice manager, general practitioner, nurse, admin team	Own practice results; other practices are anonymous. Can only view comments for their practice.
PHO	Quality manager/lead, clinical director, primary care manager	See all practices in their PHO by name.
DHB	Planning and funding, quality and risk managers, possibly DHB Alliance representative	Results only for PHOs where they are the lead DHB. Can see comments by unnamed practices in their area.
National	Commission (three people from Health Quality Evaluation) and two Ministry of Health staff	Can see all comments, although only the PHO and DHB are identifiable.