

Frequently Asked Questions: PIP QI and Data Sharing



PIP Quality Improvement (QI) Incentive

The PIP Quality Improvement (QI) Incentive commenced on 1 August 2019.

The PIP QI is a payment to general practices that participate in quality improvement activities to improve patient outcomes and deliver best practice care.

There are two components a general practice needs to meet to qualify for a PIP QI Incentive payment:

1. Participate in Continuous Quality Improvement
2. Provide the PIP Eligible Data Set to your local PHN

This FAQ factsheet on PIP QI privacy and security aims to address questions you may have around sharing data with CESP HN.

Does my practice have to share de-identified data with CESP HN to be eligible for the PIP QI?

Yes. Exceptions to this are Aboriginal Community Controlled Health Services and other organisations funded under the Indigenous Australians' Health Programme, which already provide data against the Aboriginal and Torres Strait Islander National Key Performance Indicators within existing arrangements with the Department of Health.

General practices who wish to participate in the PIP QI incentive but are unable to submit data to the PHN using Pen CAT or POLAR or choose not to use these as their data extraction tool can apply and submit a [time-limited exemption form](#) to the Department of Health for review and approval.

If approved, this exemption can give practices up until 31 July 2020 to submit the PIP Eligible Data Set. General practices are required to work in partnership with CESP HN to meet the other requirements of the PIP QI incentive without the need to share any data. For more information, see the [factsheet](#).

What does 'de-identified data' mean?

Data extracted from your practice to CESP HN is de-identified – meaning that personal, identifiable information such as a person's name, address, email address, telephone number and date of birth is removed to prevent an individual's personal identity being revealed – no identified information leaves the practice.

Furthermore, this process meets the criteria set out by the Office of the Australian Information Commissioner (OAIC) through the implementation of additional safeguards to protect patient data from possible re-identification.

What privacy and security measures are in place?

Contracts are in place with both PEN CS (for [Pen CAT](#)) and Outcome Health (for [POLAR](#)) to ensure that collection of data complies with privacy requirements and staff who handle the data are subject to confidentiality agreements.

The servers that the information is kept on comply with Australian Privacy Principles (APP) and are located in Australia.

Security standards of providers storing the information are of the highest standard and must demonstrate rigorous processes, i.e. encryption, availability, protection from physical or digital intrusion, access auditing. External security audits and penetration testing are completed by specialised external organisations.

Within CESP HN data is the foundation of our planning, decision making and operational functions. We rely on strong data governance to perform our functions effectively and maintain the trust of our data providers, data recipients and stakeholders in acquiring, handling and releasing data.

CESPHN has in place, internal data-related policies, guidelines and procedures designed to ensure compliance with the legal and regulatory environment for all staff so they have clear sources of information to perform their roles effectively and appropriately. Our Data Governance structure includes a Data Governance Committee that reports to the Executive Management Team, with reporting the CESPHN Board.

What are the data governance arrangements?

The [PIP Eligible Data Set Data Governance Framework](#) sets out the roles and responsibilities of all data custodians involved in the content, collection, use, access, aggregation, privacy and security of the PIP Eligible Data Set.

- **Local data custodians:** Participating general practices control collection, use, access, privacy and security of data at the general practice level and are designated local data custodians.
- **Regional data custodians:** Primary Health Networks (PHNs) aggregate and control collection, use, access, privacy and security of data at the regional level and are designated regional data custodians.
- **National data custodian:** the Australian Institute of Health and Welfare (AIHW) will aggregate and control collection, use, access, privacy and security of data at the national level and is the designated national data custodian of the PIP Eligible Data Set from August 2020. The details of such data sharing are yet to be finalised.

If your practice has submitted for PIP QI Exemption, you will still need to share the PIP QI data set via your software vendor software from August 2020.

Does any other organisation have access to the data?

No. Additional agreements are required to be provided by your practice for any other organisation to access your practice's de-identified data.

What will CESPHN use my practice's data for?

The aggregated de-identified data is used by CESPHN for the following purposes:

- Needs Analysis
- Population Health Planning Activities
- Project planning
- Service Mapping

The data available to CESPHN at the practice level is used to support the PHN in assisting a practice with initiatives relating to:

- Patient centred care
- Quality improvement (including accreditation and PIP QI)
- Business development

How will patients know their de-identified data is being shared?

It is a requirement to advise your patients that their healthcare information may be de-identified and used for secondary purposes, as outlined in the [RACGP Secondary use of general practice data guidelines](#). Patient privacy posters ([Pen CAT/POLAR](#)) and brochures are available to inform your patients that your practice shares de-identified patient data with CESPHN.

You can also inform your patients of sharing de-identified data by other means, for example by including patient registration sheet or patient information brochure.

What if my patients don't want their data included?

Your patients have the right to request that their information is permanently excluded from the practice's de-identified data set. Simple step-by-step guides on how to exclude the patient are available ([Pen CAT/POLAR](#))

For further clarification or support, please contact your dedicated Digital Health or Practice Support Officer allocated to your practice. Alternatively email us at digitalhealth@cesphn.com.au or practice.support@cesphn.com.au