Data Situation Audit- Privacy Impact Assessment

Data Type: GP Data- PENCS PATCAT and PATBI

Date: 27/4/2020

Reviewed 22/10/2020

Next Review 22/03/2021 (Post Primary Health Insights transition)

Risk Score: Likelihood of multi-pronged attack to access identified data- 1- Rare

Consequence of multi-pronged attack to access identified data- 5 Extreme =L1/C5 High

Privacy Impact: High

Would require a multi-pronged attack to access identified data
Impact- Extreme (5)

Likelihood- Rare (1)

Summary: All practical steps have been taken to mitigate risk and protect de identified data. It is almost impossible to use this data with another dataset outside of the practice environment to re identify. Suppression rules have been applied prior to encryption and transfer.

PenCS – PATCAT / PatBI Data Sets

Contents

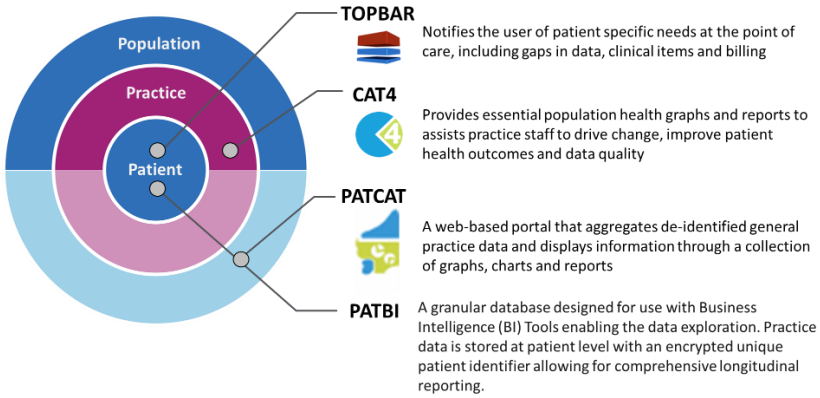
Document Control

Document Title	PATCAT_PatBI-Privacy_Impact_Assessment	Version	0.0.1

Action	By (Person / Position)	Date Finalised (Month / Year)
Created	Melissa Irvine Coordinator Health Intelligence	27/04/2020
Last Reviewed / Modified	Melissa Irvine Coordinator Health Intelligence	22/10/2020
Authorised		
Next Review Due		22/03/2020 [new hosting arrangements and new processes post primary health insights tranistion]

What are the PenCS data sets that we hold?

CAT Plus is a combination of technologies that targets three primary care layers to improve patient health outcomes; the Patient (TopBar), the Practice (CAT4) and the Population (PATCAT). The CAT Plus solution provides decision support to healthcare providers at the point of engagement (TopBar), submits general practice data for practice analysis (CAT4) and aggregates general practice data for service planning, reporting and population health needs (PATCAT).



PATCAT

The Practice Aggregation Tool for the Clinical Audit Tool (PAT CAT) is a data repository, data aggregation and reporting tool for CAT4 de-identified data extract files. It is designed to assist with population health analysis and reporting by aggregating data from many practices over time.

PAT CAT provides aggregated statistics and figures that show population health on a regional scale, yet also provides granular practice specific data. This is achieved through a collection of graphs, reports, statistics, indicators, timelines, geospatial mapping and customisable data filtering.

PatBI

The PAT BI database provides access to the data derived and submitted from CAT4 to PAT CAT, in a separate database containing granularized data requiring subsequent data modelling for use with Business Intelligence (BI) Tools (i.e. Power BI). Practice data is stored at patient level with an encrypted unique patient identifier allowing for comprehensive longitudinal reporting.

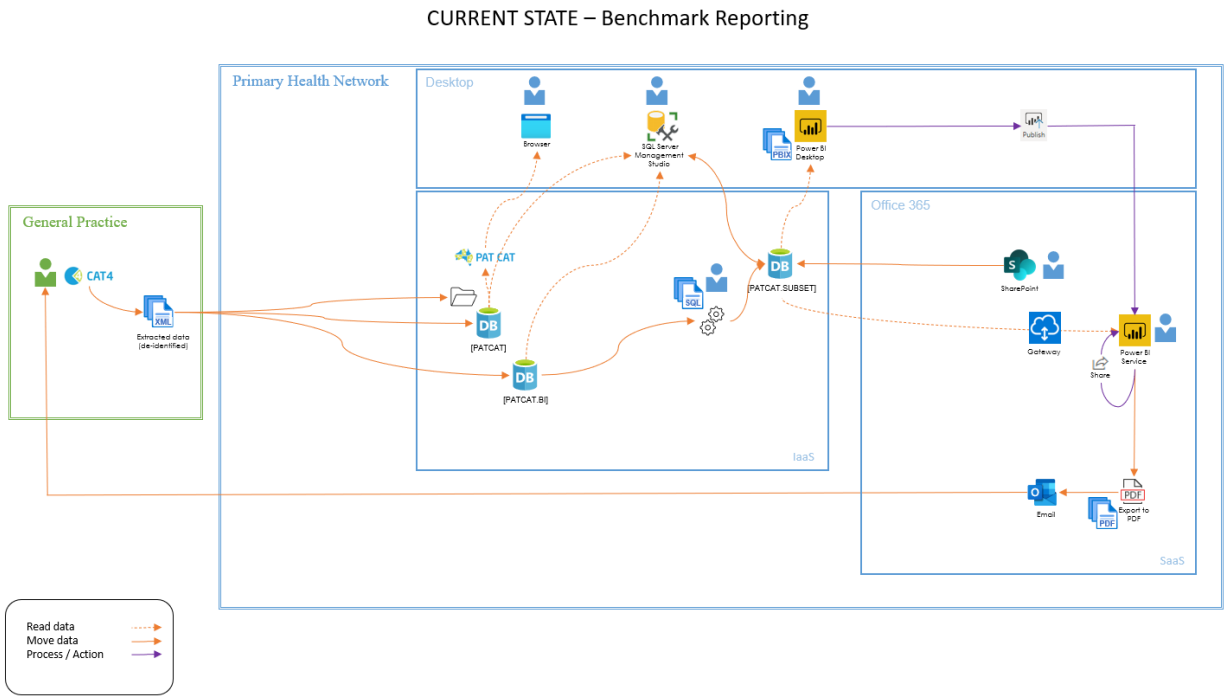
Participating General Practices upload their own patient data to the PAT CAT server in accordance with the data extraction tool agreement (DETA) provided by Central Queensland, Wide Bay, Sunshine Coast PHN.

Description of the data:

Data is received to the PHN in an encrypted csv file. The dataset includes a range of fields from the patient files pertaining to demographic, coded diagnosis, medications and clinical measures and results. For a full listing of the types of data available and specifics about field type pulled from specific practice software please see https://help.pencs.com.au/display/ds/PATCAT+USER+GUIDE.

For information about how the data is handled and contacts of the current Data Custodian and Data Steward/s please see the PHN Data Registry: Record DAT-105.

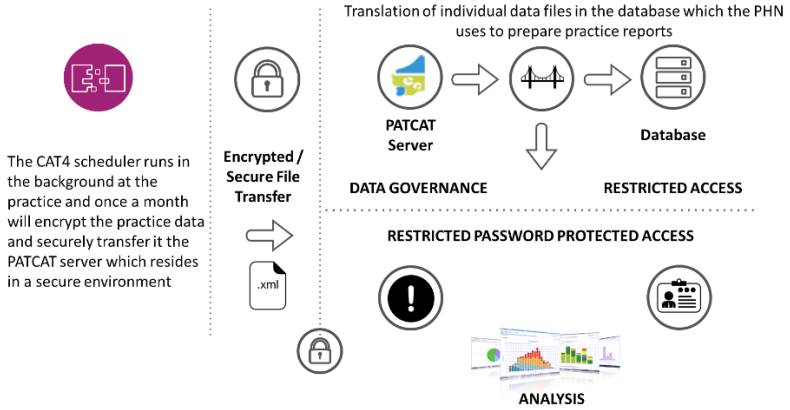
Data flows and system diagram:



Component 1: Data Description

What data are we talking about? Provide high level details.	The PATCAT database contains de-identified patient data collected from participating General Practices. A complete listing of associated data and reports available through PATCAT can be found here: https://help.pencs.com.au/display/ds/PATCAT+USER+GUIDE The PatBI database contains a granularized subset of the extracted practice data. Details on the fields available through PatBI can be found here:

<table>
<tr><td></td><td>PatBI_Schemas

Apart from being able to identify General Practices, all extracted patient data from each participating General Practice has been de-identified using an encrypted Statistical Linkage Key 581 cluster</td></tr>
<tr><td>Provide a diagrammatical view of how the data is obtained and where it is going to</td><td> 
</td></tr>
<tr><td>For each individual data environment, capture details of the following:
1. people</td><td><table>
<tr><th>Environment</th><th>People</th></tr>
<tr><td>General Practice</td><td>Practice Staff (i.e. General Practitioner, Nurse [Practitioner], Admin staff). Specific aggregated data summary reports will be provided to the practice for the purposes of Continuous Quality Improvement (CQI).</td></tr>
<tr><td>PenCS Developers</td><td>Developers from PenCS will have restricted access to the PenCS SQL servers PHNDB01P, PHNDB02P & and web server PHNWEB01P for software upgrade purposes only. Should a developer require access to the servers for either software maintenance or upgrades, a service request ticket is logged with Reliance PC'sDigital Technology Solutions (DTS), requesting the PenCS Developer have access to the servers. Once the service has been completed all access to the developer is removed, until the next request.</td></tr>
<tr><td>CQWBSC PHN</td><td>The following CQWBSCPHN roles oversee the management of the PenCS contract and General Practice engagement:

• IT Manager -IT Team
• Coordinator- Health Planning and Intelligence Team
• Data Analyst – Health Planning and Intelligence Team

The following CQWBSCPHN roles will have restricted access to the PATCAT Graphical User Interface (GUI) available at:</td></tr>
</table></td></tr>
</table>

		https://patcat.ourphn.org.au/Account/Login.aspx?ReturnUrl=%2fAccount%2fMainform.aspx and to the administration portal: https://users.pencs.com.au/ • Senior Manager - Primary Health Care Team • Senior Manager - Primary Health Care Team • Primary Health Care Support Officers - Primary Health Care Team • Primary Health Care and Commissioned Services Manager- Health Planning and Intelligence Team • Primary Health Care and Commissioned Services Coordinator- Health Planning and Intelligence Team • Data Custodian
	Reliance PC	Administrator will have access (through an approved Privileged Access Account) to the PATBI and PATCAT servers for maintenance purposes only. These are hosted by Tech Data who hold Provision of Cloud and Managed Hosting solutions including network infrastructure and secure data centre facilities for Government and Enterprise customers as identified in the Statement of Applicability ISO27001-2013 20191118 dated 18/11/2019. Certificate held on file. https://www.techdata.com/corp_assets/documents/legal/TechData-APAC-PrivacyPolicy.pdf
2. other data		CQWBSCPHN's CRM Data is used to provide analytical context, track Plan Do Study Act status for related to CQI activities, as well as monitor practice status related to various interventions and program enrolment (i.e. PIP-QI)
3. infrastructure		De-identified patient data is extracted from participating General Practices on a quarterly basis. The timing of the extraction is aligned with the PIPQI reporting cycle and orchestrated by PHN staff through the administration portal (refer to URL above). The extracted General Practice data is redirected to the hosted secure ISO27001 certified environment. In return to providing the quarterly extracts, each General Practice will be provided with a report (either in person, through video conferencing, mail attachment or direct power BI user account access) on a quarterly basis – dependent on the engagement level – developed by the Primary Health Care and Health Planning and Intelligence Team.
4. governance structures		In addition to managing the practice's enrolment into the data extraction / sharing program, CQWBSCPHN staff that require access to the PenCS environment (i.e. either to manage practices through the administration portal or for analysis purposes through the PATCAT Graphical User Interface) and application form must be completed and reviewed by both the Steward and Custodian

Component 2: Understand your legal responsibilities

With regard to the Privacy Act, the key questions are: 1. **is the data personal information or de-identified data?**	The collected data is administrative in nature and is completely de-identified. Each entry in the database is associated with a uniquely encrypted un-identifiable code specific for each practice's monthly extract.
2. **if it is de-identified data, what controls need to be in place to maintain this status?**	To maintain its de-identified status, the data set should suppress values in combination and associated with the following fields: Indigenous Status, Age and geographical region
In relation to *"Do privacy obligations still apply to de-identified data?"*, you need to identify and document how a data custodian should manage such a risk, while still using de-identified data in the ways that it is legally permitted to use it?	As per the definition of personal information (above), the data collected from General Practice, using the PenCS extraction software, does not contain any personal information. Any information which could be considered as personal, is only collected at a location level; and given the number of records per location (small practice: < 200 patients, large practice: >50,000), the ability to identify an individual is extremely remote. Analyses resulting in patient numbers less than 5 are supressed and as such are either replaced with "NA" referring to "Not Available",or excluded from the analysis all together. The following link refers to the types of reports that can be generated based on the fields that are collected from the General Practice's clinical information system. In addition to the above, the following foot notes are included in reports that are generated for external consultation: ***Disclaimer**: CQWBSCPHN is not responsible for the accuracy of the data. Please seek permission from CQWBSCPHN prior to sharing or publishing.* ***Note:** For privacy preservation reasons, the general practice data results have been supressed in cases where there are less than 5 data points.*

Component 3: Know your data

Conduct a high-level examination of your data, focussing on the data type, features, and properties. This involves: 1. **Data subjects**:	De-identified patient data is extracted from participating General Practices on a quarterly basis. The timing of the extraction is aligned with the PIP QI reporting cycle and orchestrated by PHN staff through the administration portal (refer to URL above). The extracted General Practice data is redirected to Reliance PC's secure ISO27001 certified environment. In return to providing the monthly extracts, each General Practice will be provided with a report (either in person, through video conferencing or email attachment) on a quarterly basis – dependent on the engagement level – developed by the Primary Health Care and Health Planning and Intelligence Team.
2. **Data type**:	**Information Flow:** Patient information is collected at the time of consult (or sometimes after) by General Practice staff members that are part of the patient's health management team. General Practices that choose to participate in the PHN's data sharing program or the Commonwealth's Department of Health Practice Incentive Payment Program for Quality Improvement (PIP-QI), agree to have their de-identified patient data extracted to the PenCS servers on a monthly basis. The extraction is orchestrated by the CAT4 software, provided to each general practice by the PHN. Each month the extraction file (in the form of an .xml) is generated, compressed, encrypted and sent to the PATCAT server using secure https transfer protocol. As the files from participating General Practices are received within Reliance PC's secure ISO27001 environment, the files are de-compressed and converted to Structured Query Language (SQL) enabling the encrypted, de-identified patient data to be entered into the database. Once in Reliance PC's hosted secure environment, only approved and authenticated PHN and Reliance PC's administrator will have access to the data, each of which undergo appropriate security awareness training, for the purposes of reporting and server maintenance, respectively.
3. **Variable types**:	As each clinical information system installed at the different General Practices is unique, please refer to the following mapping link, which identifies the fields that are collected from each software system. General Practices submitting data share a de-identified Clinical Audit Tool extract. These practices are able to view their extract (i.e. to see the contents) at any time by opening the CAT4 application at their practice, by selecting an extract and choosing 'De-identify Dataset' from the Tools menu as described in https://help.pencs.com.au/display/CG/De-identify+Dataset

	Additional information about what is extracted can be accessed at https://help.pencs.com.au/display/ADM
4. Dataset properties:	**De-identification of patient data** CAT4's Filtering and Anonymisation Tool (Fat Cat) is used at the General Practice to de-identify the data extracts and to "certify" the extract as de-identified. Only "Fat Cat certified" extracts are uploaded to the PHN Aggregation Tool (Pat Cat) – non-certified extracts are rejected. The Fat Cat tool creates a .dat file (discussed below) and a de-identified data file in an XML format which CAT4 subsequently compresses and sends to Pat Cat servers locations as per hosting arrangements with Reliance PC. The data transfer process uses a secure https webservice to send the compressed XML file with the General Practices (sender organisation) credentials. This needs to be initiated from within CAT4 by a logged-in user of the participating General Practice. The Pat Cat tool, installed on the Pat Cat server at Reliance PC, is configured to only receive compressed XML files that are de-identified and have been through the Fat Cat process. The transfer process confirms the sender organisation's credentials and will only accept a file from an organisation that is linked to Pat Cat. Note: The .dat file always remains at the practice and DOES NOT get sent to Pat Cat. **Identifiable data remains at the General Practice:** The .dat file generated through the extraction process by Fat Cat enables the practice staff to work with identifiable data within CAT4. Within Pat Cat the data is de-identified **Dataset size:** The datasets collected from each participating practice will continue to increase in size in an exponential manner as each monthly extract is a cumulative extraction of information added on to the previous months extract. **Dataset retention:** Neither a retention policy nor a destruction schedule is currently in place, however section 4.4.2 of the Data Sharing Agreement stipulates that the data will be retained upon until the termination of the contract with General Practice

The data itself can have properties that make the data situation more or less sensitive. Three questions capture the main points here: 1. Are some of the variables sensitive?	On their own, the following fields could be considered sensitive: Indigenous Status and Age Chronic conditions, medication prescription and pathology results in combination with the above may also be considered sensitive.
2. Are the data about a vulnerable population?	No. The data only pertains to a subset of the population that is seeking clinical consultation and chronic disease management. This population as a whole is not considered to be a vulnerable population
3. Are the data about a sensitive topic?	No. The data is collected with regards to service utilisation and is in line with gathering information to provide insights on the management of patient health status while at the same time how to improve the health system. On its own, the vast majority of the data that is being collected are not sensitive as the all of the patients are de-identified and aggregated in the context of the PATCAT database.
The properties of a dataset can potentially increase or decrease the risk of disclosure. Relevant key data properties that should be documented include: 1. Data quality:	The quality of the data is dependent on how the data is both captured in the practice's clinical software. It is for this reason that the following disclaimer is added to our reports: ***Disclaimer:*** *CQWBSCPHN is not responsible for the accuracy of the data. Please seek permission from CQWBSCPHN prior to sharing or publishing.*
2. Age of data:	The project started collecting General Practice extracts in June 2014. Each quarterly practice extract contains the entire history contain in the mapped fields. The age of the data will vary between practices and will depend on the on how long the practice has been in operation.
3. Hierarchical data – data about groups as well as individuals:	No hierarchical data apart from the practice name is being captured in this dataset
4. Time-stamped (or longitudinal) data:	The data currently collected from the PATCAT servers is conducted through the GUI filter which returns a csv file. A series of dates can be allied to these filters to obtain a longitudinal data set.
5. Population or sample data:	Only patients from the community (a section of the population) who are seeking clinical care are in this data set.

Component 4: Understand the use case

In determining the use case, you need to understand three things: 1. **Why**:	Reasons for sharing the collected data through PenCS: • Evaluation / analysis • Progress reporting • Internal reports • Publication for public consumption
2. **Who**	• Collaborative partners (intervention development) • Department of Health – for reporting purposes • Researcher(s) with ethically approved research projects • CQWBSCPHN data custodian • CQWBSCPHN project officer
3. **How**	CQWBSCPHN data technicians and analysts in the Health Intelligence and Planning Team will access and use data directly from the database presenting this information into reports in Power BI for end users. Technicians also use PATCAT access to validate queries. The preference is for end users to access reports via Power BI but non technicians from the Primary Health Care Team and Health Planning and Intelligence Team can be access and download from the PATCAT servers to CQWBSCPHN through a secure, password protected web site. Once the data is at CQWBSCPHN it is stored in a secure drive accessible only to these team members. Access to the secure drives are set up by Reliance PC at the request of Senior Mangers of the respective teams.

Component 5: Meet your ethical obligations

1. Consent	There is no third-party use of the data without the consent of the General Practice. The General Practice assumes this responsibility by signing the Data Sharing Agreement. The PenCS software platforms have been designed and structured to ensure the safety, integrity and security of patient data is compliant with the Privacy Act 1988, Privacy Amendment Act 2012 and the Privacy Regulation 2013. All data leaving the general practices is de-identified and filtered to exclude patients who have withdrawn their permission for their data to be shared for population health and reporting purposes. Practices are encouraged to follow the RACGP guidelines on privacy: "In general, a practice's quality improvement or clinical audit activities for the purpose of seeking to improve the delivery of a particular treatment or service would not be considered a directly related secondary purpose for information use or disclosure. In other words, it is likely the practice would need to seek specific consent for this use of patients' health information for clinical audit activities. To ensure patients understand and have reasonable expectations of quality improvement activities, practices are encouraged to include information about quality improvement activities and clinical audits in the practice policy on managing health information. Ideally, express consent for these activities will be obtained upon patient registration." http://www.racgp.org.au/your-practice/standards/standards4thedition/practice-management/4-2/confidentiality-and-privacy-of-health-information/ **Patient Consent:** Patients' have the option to withdraw from sharing their information at the practice level by notifying the practice. If the patient withdraws consent for their data to be shared for the purpose of the PIP-QI or secondary use, the practice can use the functionality in CAT4 to exclude them from this data

	sharing activity only. Using this feature removes the patient's data completely from any de-identified data files that CAT4 creates. This only needs to be done once for a patient, and that patient will be excluded from all future extractions. Instructions on how to opt a patient out of data sharing via CAT4, can be found here. Note: this process only excludes non-consenting patients from data extracted via CAT4. It does not exclude them from other data sharing activities that the practice might be participating in.
2. Transparency of actions	De-identified patient data will be used in an aggregated fashion to help better understand the State's health care needs and work with primary care to improve the community's health and well-being through targeted activities and interventions.
3. Stakeholder engagement	It is a result of previous stakeholder consultation that practices are participating in the data extraction program.
4. Governance	• The IT Manager is the contract manager accountable for the PenCS suite of tools, they manage the budget and risk relating to these activities. • Coordinator- Health Planning and Intelligence is the Data Custodian of the data collected through the PENCS suite of tools. • The Data Analyst- Health Planning and Intelligence(GP Data), is the system owner and the Data Steward responsible of the data collected through the PENCS suite of tools. • The Data Extraction Tool Agreement defines how the data can be used for secondary use.

Component 6: Identify the processes you will need to go through to assess disclosure risk

1. **Incorporation of your top-level assessment to produce an initial specification.**	The data collected from General Practice is already de-identified and encrypted at source (i.e. the participating General Practice), however there are still outlying possibilities where patients could be identified. To further reduce the complexity and sensitivity of the analytics / reports generated from data collected from General Practice; results which include fields such as: Age and Indigenous Status in combination with chronic diagnoses (i.e. Diabetes, COPD, Cardiovascular, Mental Health, Cancer, Musculoskeletal and Renal Impairment) and geographic regionality must not be included in the final reports if the count is less than 5. In these situations, the information is required to be suppressed by either removing the result from the final analysis or by replacing the number with "NA". The above data suppression techniques will be applied to all external facing reports and analysis, including the data summary reports specific to each General Practice. Specific reports to identify specific patients at risk can be done at the General Practice using CAT4. Additionally, the data will be handled in accordance by the guidance outlined in the Five Safe's Framework for data access: safe people, safe projects, safe settings, safe data and safe outputs
2. **An analysis to establish relevant plausible scenarios for your data situation.**	**Scenario 1**: The possibility of a General Practice Data Report being generated for the wrong General Practice (i.e. the data has been swapped with another practice) **Scenario 2**: The possibility of the wrong Data Report being accidently sent to the wrong General Practice **Scenario 3:** Mismanagement of data by the recipient of the data report (i.e. staff member at the General Practice) **Scenario 4:** Unauthorised access to the secure drive. **Scenario 5:** Power BI row level access granted to the wrong user (i.e access granted to a member of the wrong General Practice)
3. **Data analytical approaches.**	**Scenario 1:** The risk of a General Practice Data Report being generated for the wrong practice is low. The consequences, if undetected, could result in actions taken by the practice for the wrong / misinformed reasons. This is dependent on the correct mapping of the practice name to the CRM ID, which needs to be set up in both the admin portal and PATCAT's Graphical User Interface.

	Scenario 2: The chance of a report going to the wrong practice is moderate. As the data is de-identified, the risk is predominantly contained at the administrative level, with the recipient practice being able to get an understanding of a competing practice's patient cohort. The distribution of practice reports is orchestrated predominantly by the Primary Health Care team. Scenario 3: The risk of a General Practice Data Report being mismanaged in the practice is dependent on privacy and security policies implemented at each separate practice with guidelines provided by the RACGP. The consequences would be similar to those outlined in Scenario 1 Scenario 4: Access to CQWBSCPHN secure drive is managed by Reliance PC through our Identity Management processes and likelihood is low. Scenario 5: Access to CQWBSCPHN Power BI permission dashboard is managed by Reliance PC and our report technician through our Identity Management processes and likelihood is low. .
4. Penetration testing.	Security vulnerability scan over the PATCAT, PATBI and Power BI environments are conducted as per the IT Security Procedure. The above scenarios have been considered and actions outlined through mock data breach investigation.

Component 7: Identify the disclosure control processes that are relevant to your data situation

Scenario 1 - Report Generated for The Wrong Practice

1. If you need to reconfigure the environment, how would you do that?	To mitigate the risk of data being swapped with another practice both the Admin Portal, PATCAT GUI and database will be routinely validated against the CRM. The CRM is the canonical source of truth, we have a database connection to update from the CRM however the Admin Portal, PATCAT GUI are updated manually each quarter.
2. If you need to modify the data, how would you do that?	Once the swap has been identified: • The entire data report pipeline will be stopped (containment) • The problem will be assessed • All practices will be notified of the situation • A thorough review of the reporting pipeline will be undertaken These actions are in line with the OIAC's Data Breach Preparation and Response

Scenario 2 – Report Sent to The Wrong Practice:

3. If you need to reconfigure the environment, how would you do that?	To reduce the possibility of a General Practice's Data Report from being sent to an unintended recipient, The Primary Health Care Team are encouraged to present and review the report in person or through video conferencing technologies. Direct access via Power BI is also an option for highly engaged practices.
4. If you need to modify the data, how would you do that?	If a report(s) has been sent to the wrong practice, • The distribution process will be stopped (containment) • The problem will be assessed • All practices will be notified of the situation • A thorough review of the distribution process will be undertaken These actions are in line with the OIAC's Data Breach Preparation and Response

Scenario 3 – Mismanagement of The Data Report by General Practice:

5. If you need to reconfigure the environment, how would you do that?	To reduce the possibility of a General Practice's Data Report form being mismanaged (i.e. sent to an unintended recipient by internal practice staff), GPs are encouraged to follow the RACGP Guidelines to data management. If a Notifiable Data Breach occurs, refer to RACGP's "*Managing notifiable data breaches in general practice*" guidelines (https://www.racgp.org.au/FSDEDEV/media/documents/Running%20a%20practice/Security/Managing-NDB-in-general-practice-flowchart.pdf)
6. If you need to modify the data, how would you do that?	CQWBSCPHN Primary Health Care Team will remind practices to conduct regular data asset and staffing audits to ensure that their data, including the Practice Data Reports, are managed in an appropriate manner.

Scenario 4 – Unauthorised access to the secure drive.

1. If you need to reconfigure the environment, how would you do that?	This is in the case of internal staff being granted access in error. Alert Reliance PC immediately to cancel the access. Have a review of current access and using the Identity Management System get system owner to re-confirm current access requirements.
2. If you need to modify the data, how would you do that?	If a report(s) has been accessed by the wrong staff member, • The access will be stopped (containment) • The problem will be assessed • The root cause of the incorrect access will be identified • Reporting is not required as all staff are bound by our confidentiality clause in employee agreements.

Scenario 5 – Power BI row level access granted to the wrong user (i.e access granted to a member of the wrong General Practice)

1. If you need to reconfigure the environment, how would you do that?	To reduce the possibility of a General Practice's Data Report from being accessed by an unintended recipient, there is a three- step permission process. 1. Power BI access as per our identity management process granted by Reliance PC as per Senior Manager/ System Owner approval 2. Row level access providing a user to a practice by technician 3. Dedicated Primary Health Care team do an access and data validation activity before any new reports are released.
2. If you need to modify the data, how would you do that?	If report(s) access has been provided to the wrong practice, • The distribution process will be stopped (containment) • The problem will be assessed • Affected practices will be notified of the situation • A thorough review of the distribution process will be undertaken These actions are in line with the OIAC's Data Breach Preparation and Response

Component 8: Identify your stakeholders and plan how you will communicate with them

Document who your stakeholders are and what assurances you provided them with in terms of the use and protection of the data.	Stakeholders include: • General Practice Staff (i.e. Practice Principal(s), General Practitioners, Practice Nurses, Practice / Business Managers, Reception Staff) ○ Assurance has been provided to participating General Practices as to the terms of and data protection through the Data Sharing Agreement • CQWBSCPHN staff (i.e. Members of the Primary Health Care Team, Health Planning and Intelligence Team, Senior Management, Data Governance Group) • Reliance PC

Component 9: Plan what happens after you have shared or released the data

1. Keeping a register of all the data you have shared or released, including a description of the associated data environment(s).	One off reports & Research Requests: A file is created in the Outputs Log on the Data Management SharePoint Site. Routine Data Reports Generated for General Practice: A copy of the practice report will be copied to the Practice folder in the drive for archiving.
2. Comparing proposed share and release activities to past shares and releases to take account of the possibility of linkage between releases leading to a disclosure.	One off reports & Research Requests: This project will utilise the Data Register and Outputs Log managed by the Health Planning and Intelligence Team. Routine Data Reports Generated for General Practice: Restrictions to how the data can be used has been explained in the Data Extraction Tool Agreement.
3. Be aware of changes in the data environment and how these may impact on your data.	New database schemas and software functionality are expected to be released without early warning. Efforts are underway to engage with PenCS to become a beta / alpha testing site so that changes in the environment have less of an impact than they currently do. In light of receiving confirmation of the above, selected fields are used to compare the previous 3 months' worth of data to that of the most recent extract. A deviation greater than 10% of the previous months data will trigger further investigation of the newly received data extract.

Component 10: Plan what you will do if things go wrong

1. **Robust audit trail** - Document the process you would follow in the event of a possible breach.	All data breaches will comply with the procedures and guidelines outlined in the Data Breach Policy and Procedure and tracked Data Breach Register.
2. **Ensure you have a crisis managemen t policy.**	In the unlikely event that a data breach were to occur, steps outlined in the IT IT Security Procedure have been developed to ensure that CQWBSCPHN is able to deal with the incident effectively and efficiently.
3. **Ensure you have adequately trained staff.**	All members of the Health Planning and Intelligence Team involved in data processing activities associated with this data set are suitably skilled and experienced for the tasks they undertake and understand their responsibilities. The Health Planning and Intelligence Team maintain their skill sets in, and awareness of, data governance, data de-identification & cyber security by routinely undertaking training modules through Lynda.com and Microsoft Learning and Australian Cyber Security Centre training. In addition to the above subscriptions, our teams are also encouraged to undertake the online Digital Health Security Awareness Training offered through Australian Digital Health Agency: • https://training.digitalhealth.gov.au/enrol/index.php?id=31 

4. Notifiable Data Breach process.	All data breaches will comply with the procedures and guidelines outlined in the Data Breach Policy and Procedure and tracked in the Data Breach Register.