Primary Sense

Data Governance Framework

1. General Requirements

The Software Operator (currently the WA Primary Health Alliance, WAPHA, operating as Lead PHN for all Primary Health Networks using Primary Sense) must:

(a) ensure that all architecture, design, development, management, operation and use of Primary Sense complies with all approved cyber security and privacy standards, policies and procedures;

(b) comply with and enforce Primary Sense data governance policies and standards at all times, including in circumstances which require it to provide or prevent access to some or all data, including when that access is being sought by or on behalf of a PHN or General Practice;

(c) ensure that the current deployed version of the Primary Sense software is substantively the same as the version most recently covered by a Privacy Impact Assessment (PIA) with respect to the collection, storage, management, access and use of data;

(d) ensure that a suitable and appropriate Privacy Impact Assessment is undertaken and taken into consideration as part of the assessment and prioritising of any development work likely to result in a substantive change to the nature, quantity or kind of data extracted from General Practices;

(e) arrange in each Financial Year for an appropriately qualified and experienced external and independent vendor to undertake a security review and penetration test of Primary Sense, and report to the Primary Sense Project Committee how any critical and high priority findings will be urgently addressed;

(f) prepare a Summary Report of that does not contain any specific details or technical information of the findings of any security review and penetration test of Primary Sense, and any subsequent response plan developed, and provide the Summary Report to each PHN using Primary Sense; and

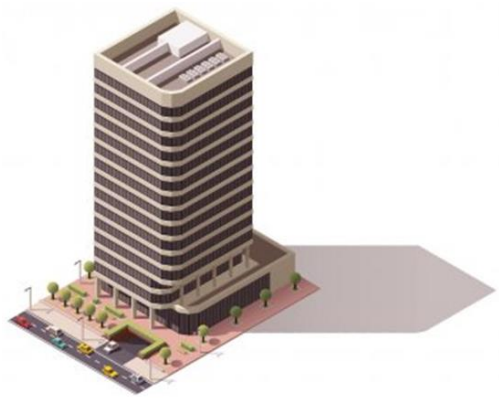
(g) include in the Primary Sense Strategy any identified potential pathways for obtaining any data governance, privacy or security certifications for Primary Sense as deemed required by the Primary Sense Project Committee from time to time.

2. Overview – Primary Sense data flows in PHI

To assist in understanding how data flows to, within and from Primary Sense and each PHN's access to that data within the hosting Primary Health Insights (PHI) platform, it is useful to use of an analogy. As with all analogies the one used below does not fully or accurately describe all aspects of Primary Sense and should not be interpreted or used as if it does, as it is only provided to assist in understanding of the data flows.

2.1 PHI as a 'shared data building'

- Prior to PHI, the PHN data landscape consisted of 29 individual, isolated and different data environments one for each PHN.
- Each of these data environments can be pictured as a separate data 'building', each with different designs, sizes, capabilities and security – even though all were intended and used for the same business purposes and used to do largely the same business activities.



- PHI was designed and built as a single, larger, more capable and secure data 'building' that is shared among PHNs.
- PHNs are co-owners of the entire PHI 'building', but each has their own dedicated and secure 'floor' – the Lockbox – in which they can store, access and use their own data.
- Inside the PHI 'building' all PHNs can access common 'floors' or services, or choose to work with selected other PHNs in more restricted-access project 'floors' or collaboration areas.
- PHI operates as a highly secure, shared data and analytics 'building', with new capabilities regularly built and released.

2.2 Primary Sense as a 'shared building service'

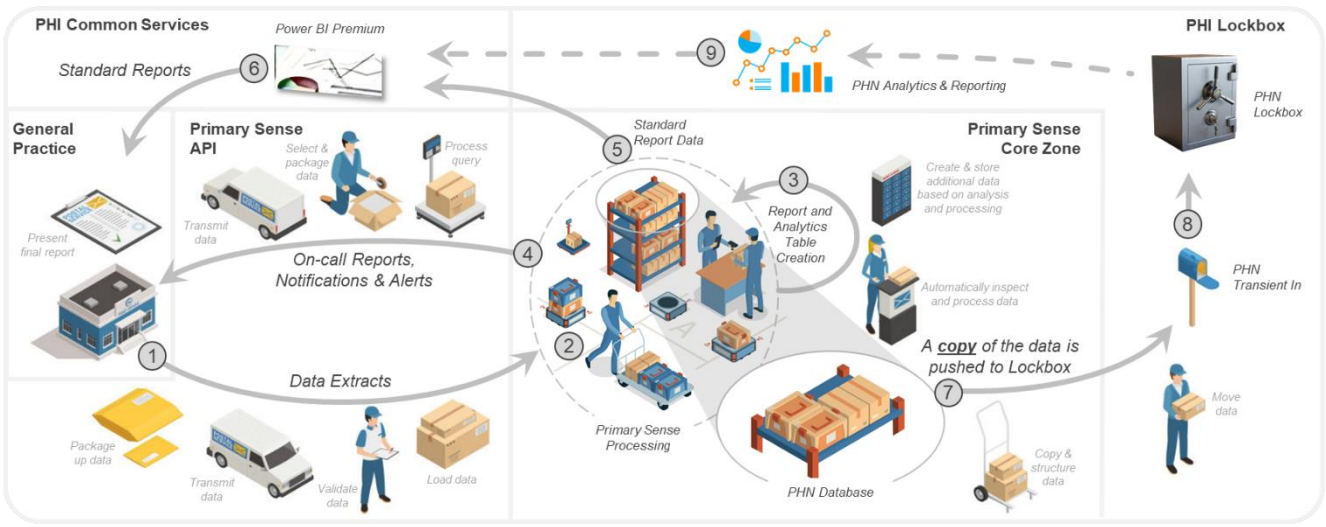
The analogy defined above can be extended by describing Primary Sense as a service available to the tenants (PHNs) of a multi-tenanted building (PHI) that operates out of its own dedicated 'service floor':

- Primary Sense has been set up as a common 'mail processing centre' for the PHI 'building' with access granted only to authorised staff.
- Primary Sense receives and processes data 'packages' received from GPs before sending 'packages' back to GPs and delivering each PHNs 'mail' (data from their GPs) to that PHN's 'floor' or Lockbox.
- The 'mail processing centre' is secure and only accessible to staff that work there, although PHN 'tenants' and GP 'package' senders be given escorted access to make sure that their 'mail' is being handled properly.

2.3 Primary Sense data flows in PHI

Using the analogy defined above, Primary Sense accepts data 'packages' extracted from GP records systems that are sent to and processed in the Primary Sense Core Zone 'mail processing centre', and then re-packages the data for delivery to each PHN's 'mailbox' on their own 'floor' for analysis and reporting.

The following diagram expands on this and begins to connect aspects of the analogy to functional aspects of how Primary Sense was designed, built, and operates:



The following notes refer to each of the steps in the data flow diagram above:

1. Primary Sense includes server software installed on each GPs' local server and is connected to their Practice Management System (PMS). On a set but configurable schedule (usually every 3 – 5 minutes), this server software:
   - Sends a request to the Primary Sense Core via the Primary Sense API asking for the exact SQL query to be run for this specific GP to extract agreed data (in line with the Data Sharing + Software License Agreement);
   - Runs the SQL query against the PMS database, including only records that have been updated or added since the last time the query was executed; then
   - Sends the data to the Primary Sense API.

   The Primary Sense API then packages and encrypts the extracted data, transmits it over the internet to the Primary Sense Core Zone, decrypts and unpacks the data, validates that the data is in the expected format, and then loads the data into waiting Data Extract tables inside the PHN's specific database in the Core Zone.

2. Inside the Primary Sense Core Zone, the extracted data is monitored and processed. This includes mapping it against standard reference tables, creating additional fields for reporting, and assessing telemetry data contained in the extract about how the locally-installed Primary Sense software is performing within the GP.

3. Dedicated processes create additional tables within the PHN's specific database for reporting and analytics. This includes stored procedures to create tables specifically for use in creating reports provided back to GPs on demand, as well as running patient data from the GP through the Johns Hopkins ACG® tool.

4. Primary Sense desktop software is installed on individual GP computers. This software calls the Primary Sense API when a medication alert or notification is triggered during a consult or a GP explicitly asks to view a report. If the report requested is intended to contain identifying data, the desktop software takes the de-identified data sent via the Primary Sense API and contacts the GP's PMS. Any identifying data is added to the report directly on the desktop, and never leaves the GP environment.

5. Some standard report tables created during Step 3 may also be intended for viewing through the PHI Power BI Premium service instead of (or as well as) through Primary Sense.

6. Reports or dashboards created in the PHI Power BI Premium service can be configured as either public (anybody with a link to the report can view the data), restricted (only users with a PHI 'guest' account – which includes the standard account for each GP during the installation of Primary Sense – can view the data) or filtered (each user can only view records they have specifically been given permission to see, such as their own GP or PHN).

7. On a set but configurable schedule (usually once a day) a data pipeline run by the Primary Sense Core Zone will take a copy of all new or updated data in each PHN's database, package it up in both 'raw' and 'structured' formats (e.g., in a proper star schema optimised for data analytics and reporting), and send it to the 'Transient In' mailbox of the PHN's Lockbox.

8. A data pipeline run within the PHN's Lockbox detects whenever new Primary Sense data is sent to the 'Transient In' mailbox, reads the data, copies it into the Lockbox, and then deletes it from the 'Transient In' mailbox.

9. As and when needed or decided, the PHN's analysts further process, analyse and report on the data. This can include creating new reports or dashboards which can be accessed by authorised GPs or other users through Power BI.

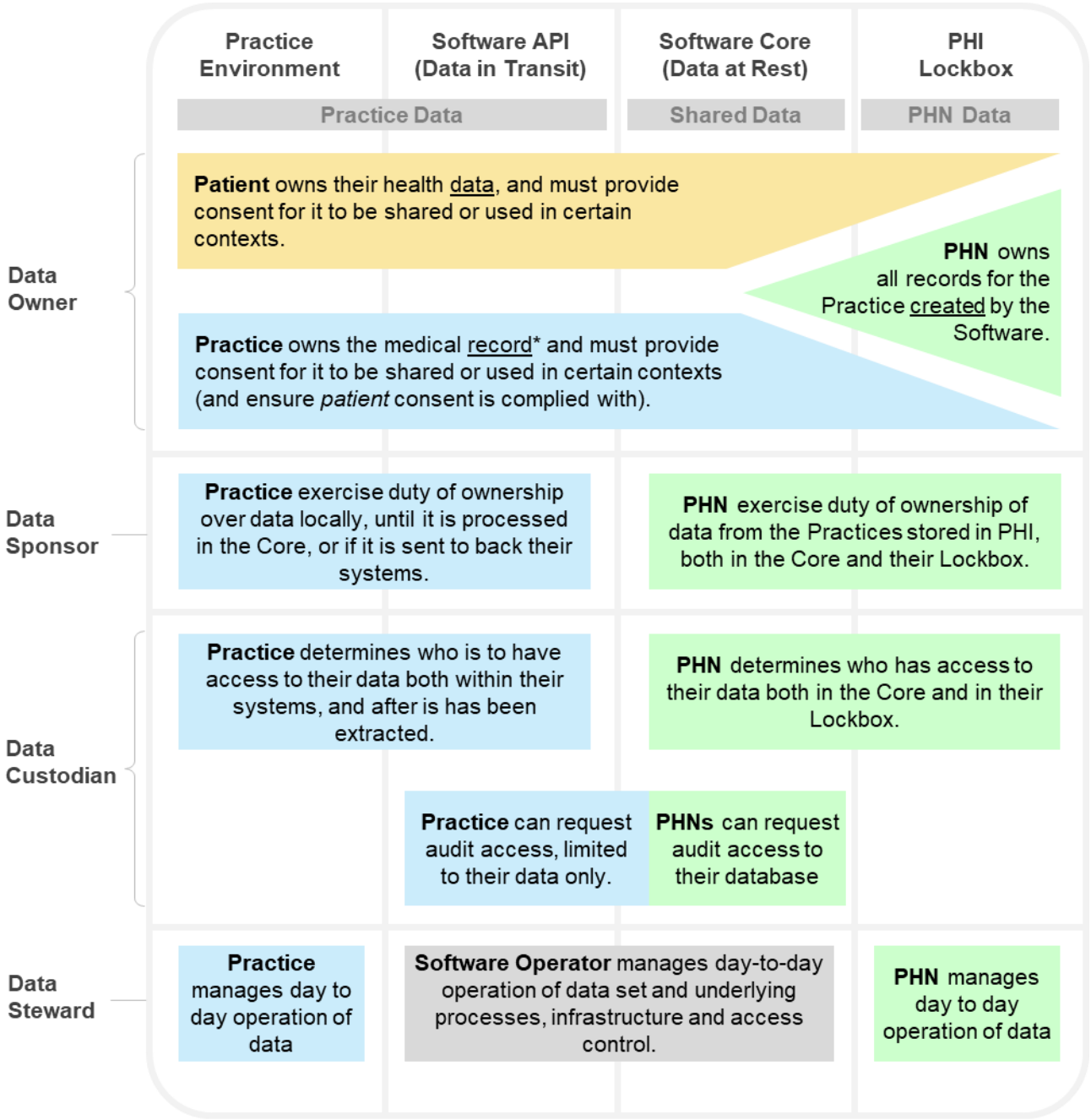
3. Data Governance Roles

The National Data Governance Framework defines key data governance roles with associated data rights and responsibilities, and which can be clarified further when placed within the context of Primary Sense as defined in the following table:

National Data Governance Framework		Primary Sense Context	
Role	Accountabilities	Role	Accountabilities
Data Sponsor	• Establish basis for a data set • Enable strategic management, governance and operation • Approve and authorise resources to manage data set • Ensure data governance is applied to the data set • Ensure compliance with relevant legislation, policies & standards • Appoint Data Custodian and ensure duties are fulfilled	**Data Owner**	• Agree to the collection and storage of the data • Provide consent and define any conditions on the sharing or use of the data
		Data Sponsor	• Undertake the duties of ownership on behalf of the Owner • Ensure compliance with any defined conditions
Data Custodian	• Ensure rules on data structure and storage are documented • Ensure data is only retained as long as it is relevant to needs • Control access to data in compliance with any conditions • Establish and maintain data quality framework for data set • Define and ensure required level of data protection and security • Ensure a process exists for responding to breaches • Appoint Data Steward and ensure duties are fulfilled • Escalate material risks and issues to Data Sponsor	**Data Custodian**	• Ensure data is collected and stored for approved purposes • Define and approve requirements for data storage • Ensure data is not retained if no longer required • Determine and approve who has access to data • Approve and monitor application of data quality framework • Ensure required data protection and security is enforced • Ensure a process exists for responding to breaches • Appoint Data Steward and ensure duties are fulfilled • Notify Data Owner of any breaches or material issues
Data Steward	• Manage data set in compliance with all conditions • Ensure up-to-date documentation on data set • Develop and maintain metadata, business rules & guides to use • Coordinate documenting business requirements for data set • Advise Data Custodian and Data Sponsor on data management • Provide feedback on data quality issues • Escalate material risks and issues to Data Custodian	**Data Steward**	• Manage data set and enforce compliance with all conditions • Ensure up-to-date documentation on data set structures • Develop and maintain metadata, business rules & guides to use • Coordinate documenting business requirements for data set • Advise Data Custodian on data management and usage • Monitor and provide feedback on data quality issues • Escalate material risks and issues to Data Custodian

3.1 Data governance roles for Primary Sense data flows in PHI

The following diagram identifies which entity or organisation has authority, access, and control over data in each of the Primary Sense Application data environments outlined in the diagram in section 2.3. The size and location of each box in the diagram defines the scope of the authority, access and control described within it.



* as per *Breen vs Williams*, which placed ownership of medical records with General Practices

The scope and roles applied to each entity or organisation is designed and intended to comply with the Data Governance Framework, and should align with guiding principles published by the Royal Australian College of General Practitioners (RACGP) on their website relating to the use of General Practice data by third parties (which from the perspective of General Practices includes the PHNs), as well as similar advice published by other peak industry bodies such as the Australian Medical Association (AMA).

3.2 Primary Sense data governance roles assignment

The data roles, access rights and responsibilities for the key stakeholder entities or organisations involved in Primary Sense data flows in PHI are summarised below:

General Practice

The GP is the **Owner, Sponsor** and **Custodian** of all data stored within, or sent to, their environment, (e.g., their practice management system) while it is within their environment as well as while it is in transit to and from their environment.

They have all rights to decide and approve what data is extracted from their systems (as well as what data can be sent to their systems) and what limitations or restrictions can be placed on the downstream use of that data. However, they must comply and require compliance with any lack or removal of consent from a patient with respect to that patient's data. As Custodian, they can request access to their data within the Primary Sense API data flows to confirm that it is being processed and secured in line with their agreements and decisions.

They are also the **Steward** of the data while it is within their own environment, and have the responsibility for identifying and enforcing any access rules, including those related to a patient's consent or lack thereof.

Software Operator (Lead PHN) / Primary Sense Team

The Lead PHN is never the Owner, Sponsor or Custodian of any General Practice Data or PHN Data. They have no rights to decide or determine who has access to any data, unless those rights have been specifically conferred on them by a GP or PHN in their role as Steward.

The Primary Sense Team specifically within the Lead PHN is the **Steward** of all General Practice Data in transit through the Primary Sense API and of all Primary Sense Data. They are responsible for enforcing access rights and protecting the privacy of all parties to all agreements related to Primary Sense. As Steward, they must comply with any formal request from a Custodian to undertake an audit (formal or informal) of that Custodian's data, so that the Custodian can retain confidence that their data is being stored, processed and secured in line with the agreements and decisions they have made.

The Lead PHN is the **Custodian** of Primary Sense Reference Data (data or algorithms provided under license by a third-party for use in processing GP data into Primary Sense Data) and is the **Owner** of any mapping data created specifically for Primary Sense.

PHN

The PHN is the **Owner, Sponsor** and **Custodian** of all data sent by "their" GPs only after the point at which it has been processed into the Primary Sense Core Zone and becomes Primary Sense Data, as well as all data packaged and sent to their Lockbox as PHN Data. The PHN must comply with any conditions on the use of data imposed by a GP in a Data Sharing +Software License Agreement or indicated within the Consent provisions of Primary Sense.

The PHN has all rights to decide and approve how much of their data is sent to their Lockbox, and who is to be provided access to their PHN Data, but do not have unrestricted access to their data in the Core Zone, as this would unacceptably reduce the security and privacy of every other PHN's data stored within that Zone. As Custodian, they can request access to their data within the Core Zone to confirm that it is being processed and secured in line with their agreements and decisions.

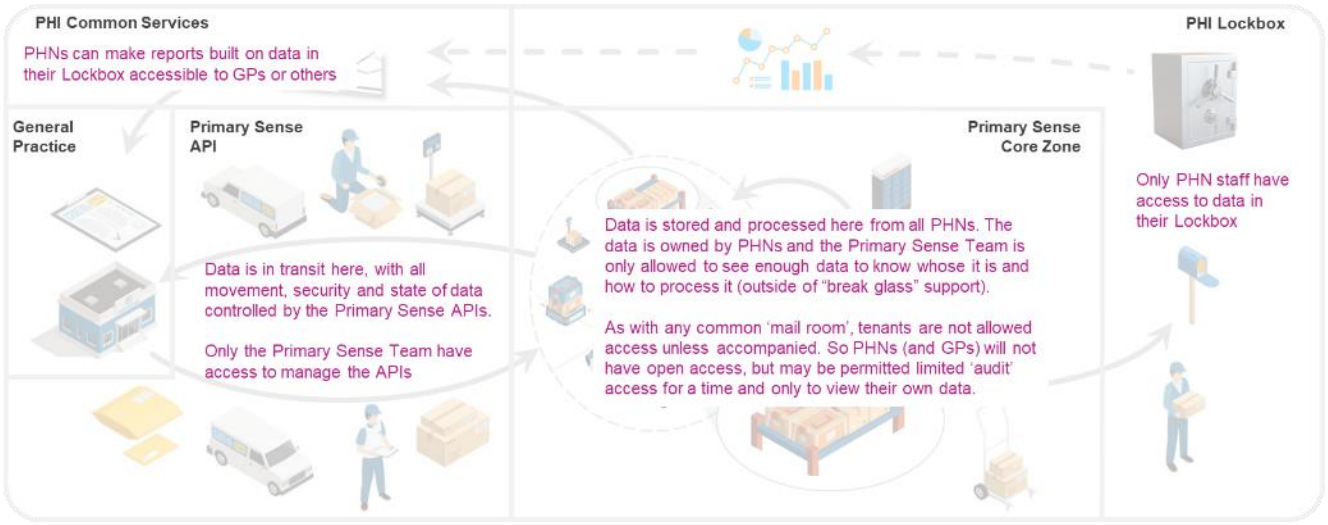
They are also the **Steward** of their PHN Data while it is within their Lockbox and have the responsibility to enforce all access and usage rules.

4. Data Sharing

Before Primary Sense can be downloaded and installed by a GP, that practice must sign a Data Sharing + Software License Agreement with the PHN.

5. Data Access and Security

To ensure that the required data governance can be effectively implemented the level of access and control over data (the 'packages' in the analogy from section 2) being moved through or stored within the various data environments within Primary Sense are clearly established. The following diagram provides an overview aligned to the analogy defined in section 2.3:



The level of access to data required by each entity or organisation is described below:

Practice Environment	Software API (Data in Transit)	Software Core (Data at Rest)	PHI Lockbox
Patient can only get access via their GP			
Practice has full access.	**Practice** can get supervised, time-limited access to their records in data streams only, for compliance audit purposes.	**PHN** can get supervised, time-limited access to their database only, on request, for compliance audit purposes.	**PHN** has full access.
Software has limited read-only access	**Software** has full access to read and write data.		**Software** has limited write-only access
	Software Operator has access to manage data flows and processes, with 'break glass' access to data only if needed.		

In the above diagram, 'Break glass' access refers to an administrator account that has sufficient privileges to view data or take an action but can only be used in an emergency situation or if specifically requested by a Data Custodian or Sponsor.

5.1 Data access by Software Operator

Since the Lead PHN controls access to Primary Sense, the degree of access that accounts used by the Primary Sense Team to different types of data must be clearly articulated. The following table provides that clarity.

Account access to data within the Primary Sense Core Zone:

Primary Sense Data Components	Primary Sense Application Accounts	Primary Sense Team "Break Glass" Accounts	Primary Sense Team Administrator Accounts	Primary Sense Team Standard Accounts	Other PHN (inc. Lead PHN) Staff
Metadata *(e.g.: table and field names, data formats, data volumes, etc.)*	**Full Access**	**Read Access**	**Read Access**	**Read Access**	**No Access** *(Audit Access to own data only on request)*
Telemetry Data *(e.g.: data records added or updated, tables and fields specific to API performance activity or system health)*	**Full Access**	**Read Access**	**Read Access**	**Read Access**	**No Access** *(Audit Access to own data only on request)*
Mapping Data *(e.g.: fields in GP data used for mapping against reference data sets)*	**Full Access**	**Read Access**	**Read Access**	**No Access**	**No Access** *(Audit Access to own data only on request)*
Reference Data *(not GP or PHN data – only third-party sourced or created by or for project)*	**Full Access**	**Read Access**	**Read Access** *(plus Scripted Write Access via Change Management)*	**Read Access**	**No Access** *(All PHNs access only via copies in Common Zone)*
All Data *(all fields, all tables)*	**Full Access**	**Read Access**	**No Access**	**No Access**	**No Access** *(Audit Access to own data only on request)*