Queensland Health

User access management

Queensland Health Guideline

QH-GDL-469:2021

1. Purpose

To support the effective management of information and the applications that support the functions of Queensland Health, implementing procedures and practices to maintain appropriate authorised user access is critical.

The purpose of this guideline is to support the standardisation of processes and practices to authorise and monitor user access to applications across Queensland Health. This guideline supports Application Custodians[1] with their responsibility to ensure a standardised process is in place to authorise and monitor user access.

This document is intended as a general information source to guide employees in developing standardised user access management processes to authorise and monitor user access. The guideline needs to be considered in conjunction with other Queensland Health and Department of Health policies, procedures, and guidelines, with particular reference to the *Use of ICT services and devices policy*, *Use of ICT services and devices standard and supporting standards.*

2. Scope

2.1. In scope

Compliance with this guideline is not mandatory, but sound reasoning must exist for departing from the recommended principles within the guideline.

This guideline:

- Includes access to applications (clinical and non-clinical) managed by Queensland Health.
- Applies to all staff within Queensland Health. Staff is defined as employees, students, interns, volunteers, contractors, consultants, Board Members, and managed service providers working for Queensland Health. Queensland Health consists of:
    - the Department of Health, and
    - Hospital and Health Services.

[1] Department of Health, *Data and application custodianship roles and responsibilities*, pg. 12.

2.2. Out of scope

Excluded from this guideline:

- Data access management.
- Technical controls or requirements.
- User access management process for those external to Queensland Health.

3. Related documents

Standards, procedures, and guidelines

Queensland Government

- Queensland Government Enterprise Architecture:
    - Authorised and unauthorised use of ICT services, facilities and devices guideline
    - Information access and use policy (IS33)
    - Information asset custodianship policy (IS44)
    - Information security policy (IS18:2018)
    - Use of ICT services, facilities and devices policy (IS38)

Queensland Health

- Access control standard QH-IMP-484-4:2021
- Audit and recordkeeping standard QH-IMP-484-9:2021
- Data and application custodianship policy QH-POL-469:2019
- Data and application custodianship standard QH-IMP-469-3:2019
- Collaboration platforms standard QH-IMP-484-6:2021
- Enterprise information, communication and technology (ICT) governance Health Service Directive QH-HSD-052:2019
- External access standard QH-IMP-484-5:2021
- Information access, use and disclosure standard QH-IMP-484-2:2021
- Information security policy QH-POL-468:2019
- Information sharing guidance documents and templates
- Monitoring and reporting standard QH-IMP-484-7:2021
- Research ethics and governance Health Service Directive QH-HSD-035:2013
- Training, awareness and disciplinary procedure standard QH-IMP-484-8:2021
- Use of Email standard QH-IMP-484-3:2021

- Use of ICT services and devices policy QH-POL-484:2021
- Use of ICT services and devices standard QH-IMP-484-1:2021

Department of Health

- Administrative privileges standard QH-IMP-066-3:2015
- Data and application custodianship roles and responsibilities
- Inactive account management standard QH-IMP-484.11:2021
- Research management policy QH-POL-013:2022

4. Guideline for user access management

User access management involves managing who can use, change, or view applications and information within these applications and the circumstances in which such access is permissible.

Control measures are necessary to ensure that only authorised users can obtain access to applications and information contained within applications. Access control measures manage the admittance of users to applications by granting users access only to those components of an application that they require to complete their job role.

User access requirements have an ongoing need to adjust due to changes in the access environment. For example, personnel joining and leaving, staff moving between roles, and the introduction of new applications into the organisation. Consequently, Queensland Health must have well-defined and documented measures in place for monitoring user access, and effective processes in place for enabling and disabling access.

4.1. Guideline principles

The following controls for managing user access to Queensland Health applications are based on the following principles:

- **Need to know:** Users will be granted access to applications that are necessary to fulfil their roles and responsibilities.
- **Least privilege:** Users will be provided with the minimum access privilege necessary to fulfil their roles and responsibilities.[2]
- **Review user accounts and access:** Regular review will occur to determine the user accounts and access privileges assigned to users are appropriate.
- **Deactivate user accounts:** Remove user access when it is determined that a user account is no longer required.

[2] Queensland Audit Office, 2019, *Access controls for information technology systems*.

4.2. Authorised access

The establishment of defined roles, responsibilities, and user access requirements will ensure that authorised users are granted appropriate access levels to applications and information within these applications, which will enable them to perform in their roles, while also ensuring appropriate levels of security are maintained.

To prevent unauthorised access to Queensland Health applications and information, access rights and privileges should be assigned based on a users job classification, role and/or function. Users must only be given access to applications that are necessary to perform their required role.

4.2.1. Application custodianship

The Queensland Health *Data and application custodianship roles and responsibilities* document defines roles and responsibilities in relation to the custodianship of data and applications in Queensland Health.[3]

The Application Custodian position has overall accountability and responsibility for decision making in relation to the ongoing development, management, compliance, care and maintenance of an application to support business needs. Application Custodians must also ensure a standardised process is in place to manage user application access.[4]

The Application Manager is responsible for the day-to-day management of an application including the planning, development, compliance, installation, configuration, maintenance and support of an application. This includes managing application access in accordance with Application Custodian guidelines.[5]

4.2.2. Authorisation

Only persons that are authorised by an Application Custodian or correct delegate are to be provided access to an application or information.

An Application Custodian may develop and implement a delegations framework[6] permitting the delegation of specified responsibilities to appropriately qualified staff. A delegations framework ensures that the most appropriate individuals (officers) can act autonomously to make decisions on behalf of the Application Custodian if required. The correct

[3] Queensland Health, *Data and application custodianship roles and responsibilities*, pg.4.

[4] Department of Health, *Inactive account management standard.*

[5] Queensland Health, *Data and application custodianship roles and responsibilities*, 3.2 Application Manager responsibilities, pg. 15.

[6] Queensland Health, *Data and application custodianship roles and responsibilities*, 2.3 Delegations framework, pg. 10.

delegate with delegated authority must be a senior officer with a suitable level of authority to endorse a user access request.

An Application Custodian seeking to implement a delegation framework is responsible for the development, management and review of the delegations framework as outlined in the *Data and application custodianship roles and responsibilities* document.

Templates to assist in the implementation of a delegation framework are available on the Health Informatics Services (HIS) Data and application custodianship QHEPS site.

4.3. Authorised users

User accounts will only be created when an individual has been registered as an authorised user. All users are required to be authorised by a correct delegate prior to accessing Queensland Health applications. A person that has received authorisation is considered to be an **authorised user**.[7]

For further information in relation to requirements for authorised use, refer to the Queensland Health *Use of ICT services and devices policy*, *Use of ICT services and devices standard*, *Access control standard*, and *Information access, use and disclosure standard*. The requirements for authorised users may also include authorisation under legislation e.g. the *Public Health Act 2005* (Qld) or the *Hospital and Health Boards Act 2011* (Qld).

Prior to authorising any user access request, the correct delegate will need to consider the specific requirement.

The process of access to applications and information may differ between users internal and external to Queensland Health. The scope of this guideline is for user access to applications for staff internal to Queensland Health. However, the following sections, 4.3.1 and 4.3.2, provide information in relation to access to information under certain circumstances for users external to Queensland Health.

4.3.1. Access to health information by external researchers

In general, there is no legal authority for researchers, external to Queensland Health, to directly access a Queensland Health information system, whether or not by secure means, for research purposes if the system holds information that has the capacity to identify an individual patient.

Chapter 6, Part 4 of the *Public Health Act 2005* (Qld) (PHA) establishes a process by which a person, including external researchers, may apply, and be approved, to be given health information held by Queensland Health

[7] 'Authorised user' as defined in the Queensland Government Glossary for government.

for a specific research study. The PHA enables appropriate Queensland Health employees to extract and give, on conditions, the relevant information to applicants whose PHA application has been approved by the delegate in the Office of Research and Innovation (ORI) in Queensland Health. Importantly, the approval does not grant to an applicant direct access to Queensland Health information or information systems. ORI administers PHA applications and further information about the PHA application process, including an application form, is available at the ORI website.

Further general information regarding the use of Queensland Health information for research purposes can be found in the Research, ethics and governance Health Service Directive. ORI, the relevant Data Custodian or local HHS Research Governance Officer, may also be contacted for additional guidance.

4.3.2. External service providers and prescribed health practitioners

Section 161A of the *Hospital and Health Boards Act* (Qld) provides, in general terms, that the Director-General, Queensland Health, may authorise an external service provider, or person engaged by an external service provider, to access an information system that holds information that has the capacity to identify an individual patient (that is, 'confidential information' as defined in the Act). Authorisation may be granted, on conditions, only if the access is necessary to enable an external service provider to provide a 'health service' (as defined in the Act) under an agreement between the Director-General, Queensland Health, or a Service and the service provider.

Section 161C of the HHB Act, provides, in general terms, that a 'prescribed health practitioner' (as prescribed in the *Hospital and Health Boards Regulation 2012* (Qld)) may access a 'prescribed information system' (currently only 'The Viewer' is prescribed in the Regulation) to facilitate the care or treatment of an individual. In addition to complying with the prohibitions on disclosure in Part 7 of the *Hospital and Health Boards Act* (Qld), the practitioner must comply with all conditions prescribed by the Regulation in relation to accessing a prescribed information system and any information contained in the system.

4.4. Non-compliance

The information and the applications that support the functions of Queensland Health contain confidential, sensitive, and critical information. Threats to this information and applications can be both internal and external to Queensland Health. Robust

access control mechanisms are required to mitigate the risk of unauthorised access to confidential information to achieve integrity, confidentiality, and accountability.[8]

All staff must be appropriately authorised prior to accessing and using ICT services and devices. Non-compliance represents a risk to Queensland Health's information, systems, and reputation. For further information in relation to the conditions that staff must abide by as an authorised user, see the Queensland Health *Access control standard*, *Use of ICT services and devices policy* and *Use of ICT services and devices standard*.

5. Requirements

5.1. Access to Queensland Health applications

Access to Queensland Health applications is restricted to authorised users. The requirements and process for establishing new user access may differ between each application, based on specific legislation that may govern the application or the information held in it and the procedure determined by the Application Custodian.

When requesting access, there is a requirement to understand what type of access is required and the correct process to request user access. There are generally two processes that may be relevant for a user to request access to an application:

1. Request access through the Online IT Support portal[9]. Refer to **Appendix A** for further details. Please note that Access Manager is a new solution that manages IT access for Queensland Health staff. Access Manager is available via the Online IT Support portal and is being progressively implemented across the state. Access Manager will eventually replace the Online Provisioning System. Sites that do not have Access Manager are to use the Online Provisioning System. Further details are available in Appendix A.
2. Request access through an Application Manager via the User access application form (or equivalent) as determined by the Application Custodian.

Requests to gain access to an application will require authorisation, generally requiring the capture of personal details to ensure the access that is provided is appropriate for a users' duties[10]. The level of access a user has is generally determined by their job role. Often, staff will require training to be completed before full access is granted.

[8] *Operation Impala – Report on misuse of confidential information in the Queensland public section,* pg. 57.

[9] This includes access through ServiceNow to applications and software categories and directly through the Online Provisioning System.

[10] Note – if personal information is collected directly from an individual, a privacy notice is required. For more information regarding privacy notices refer to the fact sheet – Privacy notices - general obligations and draft template

Users are to check the process for each application for which access is required. There should be procedures for each application that details the process for the creation and management of user accounts. Users can only gain access to applications by submitting an appropriately authorised form, and where required, completing the relevant application training.

For example, access to the Consumer Integrated Mental Health and Addiction (CIMHA) application requires the completion of a CIMHA New Users Access Form. Access will only be granted upon appropriate authorisation and completion of adequate training for the application.

Shared or non-standard accounts should be disabled or removed. Any exceptions must be requested and managed in accordance with the Queensland Health *Access control standard*.

Requests for special accounts and privileges (such as vendor accounts, application and service accounts, system administration accounts, test accounts and external access) require the completion of an online form through the Online IT Support portal or Access Manager.

5.2. Limited user access

The concept of least privilege (as described in section 7 Definitions) is extended to specific access criteria such that a user is only granted access to information or resources when certain conditions are met.

For users who are employed on a temporary (short term) basis, access should only be provided for the projected length of time of employment. Some examples include:

- Single shift (e.g., casual clinician)
- Employee on secondment
- Intern/student
- Volunteer.

Refer to the *Queensland Health Access control standard* for further information regarding managing user access.

5.3. Account privileges

Account privileges are an authorisation, or a set of authorisations, which allow users to complete specific tasks associated with their role. Account privileges can be managed (restricted) based on a wide range of criteria, which include (but are not limited to) the following:

- Identity: Users are provided access based on their identity.
- Roles (not positions or titles): Users are assigned access privileges commensurate with their job requirements.
- Location: Users are assigned access privileges based on their physical location (site).

- Time/timeframe: Users are assigned access privileges based on a specific time or timeframe that access is required. For example, allowing use of an application during business hours only, or allowing temporary access to an application for a user on secondment.
- Transaction: Users are assigned access based on a specific action. For example, allowing access to view details relating to an application to respond to a query. The access will be revoked once the query has been finalised.
- Access mode: Limit a users' mode of access. e.g., providing read-only access as opposed to read/write/create.[11]

Where an employee is absent for extended periods (e.g., extended leave, secondment), the user access privileges provided for their substantive role should be temporarily disabled until their return.

5.4. Administrative privileges

Administrative/privileged access is any access where the user can bypass established system controls. This includes, but is not limited to, users responsible for providing system administrator services, maintenance and/or user support.

Although privileged access implies a degree of trust in a user being granted such access, core principles such as 'least privilege' and 'need to know' should continue to be applied. Administrative privileges must be strictly limited and must only be granted where there is an identified and authorised need for the privileges to perform the role.[12]

Privileged access procedures are subject to the additional requirements including, but not limited to:

- Administrative privileges must be assigned to a separate user account. For example, if assigned a privilege account, the non-privileged user account must be used for standard activities and the privileged account only used when required to perform tasks requiring administrative privileges.
- Documented procedures must be in place to record and capture all administrative accounts.
- All changes to accounts, including administrative privilege accounts, should be logged and auditable.

For further information in relation to administrative privileges, refer to the Department of Health *Administrative privileges standard* and Queensland Health *Access control standard*.

[11] Trusted Information Sharing Network, 2008, *Trusted Information Sharing Network for Critical Infrastructure Protection*.

[12] *Queensland Health Access control standard*, 4.5 Administrative/Privileged account control requirements, pg. 4.

5.5. Change/revoke user access

All authorised users that are granted access to applications have an obligation to ensure they only access information that is necessary for and consistent with the performance of their role and as approved by the correct delegate.

User access requirements will regularly change as a result of role changes, movement between roles, conclusion of contract/service, conclusion of project, and cessation of employment. User access to applications will need to be reviewed and updated to reflect the changes.

The correct delegate is to manage the movement of employees (including temporary employees, contractors, and consultants) and other organisations (under their control) that have access to Queensland Health applications and the information within these applications, to ensure that only authorised users have access.

Changes to user access for a Queensland Health application should be performed by following the relevant procedures for modifying or terminating user access privileges. Amendments to specific applications, including revocation, will generally require additional authorisation and completion of specific application forms.

For amendments to access to applications (including revocation), use the Online IT Support portal or Access Manager, or contact the relevant Application Manager as described in section 5.1.

5.6. User account and access reviews

Application Custodians are responsible for ensuring a standardised process is in place to authorise and monitor user access, and for ensuring guidelines are set around authorised access to ensure that role changes, such as a promotion, transfers, and separations are correctly reflected in all applications. Processes should include activity reporting and monitoring for high-risk applications.

A user account and access review will determine the access rights and privileges assigned to an application are consistent with business objectives and security principles. A review may also:

- Identify any unnecessary user access rights and privileges that have been assigned to users.
- Identify inactive accounts or excessive access privileges.
- Detect inconsistent or unauthorised use of administrative privileges.
- Detect inconsistent or unauthorised use of access rights to all information and/or applications.
- Allow for remedial action to be taken in a timely manner to resolve issues identified.

The following are some examples of user accounts with inconsistencies:

- An active account assigned to external contractors, vendors or employees that no longer work for Queensland Health.
- An active account with access rights for which a user's role and responsibilities do not require access. For example, a user that does not have authority or responsibility to approve expenses should not have access to approval permissions within a financial application.
- Administrative rights or permissions (including permissions to change the security settings or performance settings) granted to a user who is not an administrator.
- Unknown active accounts.

User access reviews should be documented and retained for auditing purposes. Application Custodians can create their own specific procedures for the review of user access accounts for their application and this may include submission of user access reviews to governance bodies. Tasks typically executed during an access review include:

- Obtaining user account lists and corresponding access rights.
- Reviewing assigned access rights against staff roles and required access rights.
- Identifying unnecessary privileges for removal.
- Obtaining audit trails and user access logs to check for changes to staff roles and job functions.
- Identifying anomalous or unauthorised access to data or functions.

User account and access reviews should be performed at least quarterly.[13] Application Managers may consider performing a review on a more regular basis. Contact can be made directly with authorised users to confirm whether their access and privileges are current or where changes need to be made. **Appendix B** is an example of a form that could be adapted and used as part of a review. Where users do not respond by the due date, access can be revoked.

For further information in relation to user account and access reviews, refer to the Queensland Health *Monitoring and reporting standard*, *Access control standard* and *External access standard*.

5.7. Training and awareness

The correct delegates are to ensure that employees (including temporary employees, contractors, and consultants) receive appropriate user access training and awareness prior to being granted authorised user access to the specific applications to which they require access to.

[13] *Queensland Health, Access control standard,* 4.7 Access reviews, pg. 6

A user may need to undertake additional training for an application before access will be granted. Some applications require training prior to the commencement of duties. Training requirements will differ between applications.

In general, all training and awareness should include:

- **Responsibilities of authorised users**: Employees should understand acceptable use of applications and also be aware of access control restrictions such as the 'need to know' requirement, and the reasons behind the restrictions. This includes any requirements, including prohibitions in use and disclosure, that is imposed by legislation. The user acceptance notice will ensure the user is informed of their responsibilities and requirements when accessing the application.
- **Information security, confidentiality and privacy awareness:** Employees should understand the need to protect Queensland Health information and applications from threats and reduce risks from unauthorised access, use, disclosure, disruption, modification, perusal, inspection, recording, destruction, damage, fraud or a beach of privacy or confidentiality.
- **Data and application custodianship:** Employees should understand and accept data and application custodianship requirements to ensure that data and information are managed throughout their lifecycle and are accessible to authorised users.
- **Training on specific applications**: Employees should undertake training on specific applications to ensure they have the appropriate knowledge and skills to operate an application effectively and in line with business requirements.

For further information in relation to training and awareness, refer to the Queensland Health *Training, awareness and disciplinary procedure* standard.

6. Definitions

Term	Definition / Explanation / Details	Source
Access authorisation	The system controls and surrounding processes that provide or deny parties the capability and opportunity to access systems (i.e., gain knowledge of or to alter information or material on systems). In practice, the act of authorising access usually occurs after authentication has been successful. Authentication checks if the party is who they claim to be. Access authorisation checks what the party is allowed to do.	Queensland Government Glossary for government
Access control	The process of granting or denying requests for access to information and systems. Can also refer to the	Department of Health Cyber Security terms and definitions

Term	Definition / Explanation / Details	Source
	process of granting or denying requests to enter facilities.	
Administrative/Privileged access	Administrative/ privileged access is defined as a level of access above that of a normal user. This definition intentionally allows the flexibility to accommodate varying systems and authentication mechanisms. In a Microsoft Windows environment this includes members of the Power Users, Local Administrators, Domain Administrators and Enterprise Administrators groups. In a traditional UNIX or Linux environment this includes users with root level access. In an application environment this includes users with system administrator roles and responsibilities.	Department of Health Administrative privileges standard
Application	A software system deployed by the agency which has part of an agency's business process embedded with it.	Queensland Government Glossary for government
Application Custodian	A position designated with overall accountability and responsibility for decision making in relation to the ongoing development, management, compliance, care, and maintenance of an application to support business needs.	Queensland Health Data and application custodianship roles and responsibilities
Application Manager	A position designated with responsibility for the day-to-day management of an application including the planning, development, compliance, installation, configuration, maintenance, and support of the application.	Queensland Health Data and application custodianship roles and responsibilities
Authorised use	Use by individuals who have received authorisation before operating the relevant device or service and agreed to abide by the policies, guidelines, and local practice arrangements for use of the relevant facility or device, and who have appropriately acknowledged this agreement where required.	Queensland Government Glossary for government
Authorised user	Users who have received authorisation before operating the relevant device or service and agreed to abide by the policies, guidelines,	Queensland Government Glossary for government

Term	Definition / Explanation / Details	Source
	and local practice arrangements for use of the relevant facility or device, and who have appropriately acknowledged this agreement where required.	
Confidential information	Confidential information as defined by relevant Queensland legislation which provides privacy and confidentiality protections for personal information.	*Hospital and Health Boards Act 2011* (Qld) *Information Privacy Act 2009* (Qld) *Public Health Act 2005* (Qld)
Data Custodian	A position designated with overall accountability and responsibility for decision making in relation to the data set, data collection and/or application allocated and the ongoing capture, compliance, development, management, care, and maintenance of data to support business needs.	Queensland Health Data and application custodianship roles and responsibilities
Data Manager	A position designated with responsibility for the day-to-day capture, management, maintenance, operation, compliance, interpretation, and supply of data.	Queensland Health Data and application custodianship roles and responsibilities
External service provider	External service provider means an entity providing a health service under an agreement between the chief executive or a Service and the entity.	*Hospital and Health Boards Act 2011* (Qld)
ICT services and devices	ICT services and devices include computers (including mobile and handheld devices); telephones (including mobiles and smart phones); paging systems; BYO devices connecting to the Queensland Health network; instant messaging services; removable media; radios or other high frequency communication devices; television sets; digital or analogue recorders (including DVD and video); cameras; photocopiers; facsimile machines; printers (and other imaging equipment); electronic	Queensland Health Use of ICT services and devices policy

Term	Definition / Explanation / Details	Source
	networks; internet; email; web mail; fee-based web services; videoconferencing equipment; collaboration platforms; ICT enabled medical devices; satellite broadcasting and ICT enabled monitoring systems.	
Information	Information is any collection of data that is processed, analysed, interpreted, classified, or communicated in order to serve a useful purpose, present fact, or represent knowledge in any medium or form. This includes presentation in electronic (digital), print, audio, video, image, graphical, cartographic, physical sample, textual or numerical form.	Queensland Government Glossary for government
Least privilege	A basic principle in information security that entities (e.g., people, processes, devices) should be assigned the fewest privileges consistent with their assigned duties and functions to protect information and increase system resiliency. For example, the restrictive Need-to-know approach defines zero access by default and then opens security as required.	Digital Policy Glossary
Prescribed health practitioner	(a) A relevant health practitioner, other than a person mentioned in section 139A (1), who is prescribed by regulation; or (b) a person who was a relevant health practitioner mentioned in paragraph (a).	*Hospital and Health Boards Act 2011* (Qld)
Prescribed information system	Means an information system prescribed by regulation.	*Hospital and Health Boards Act 2011* (Qld)
User group	An ICT user group shall be used to manage access to specific application in an ICT environment by allowing access to only authorised personnel. An ICT user group (often referred to as workgroup in Novell environment) can refer to a group in the following environment but is not limited to:	Digital Policy Glossary

Term	Definition / Explanation / Details	Source
	• Enterprise active directory • Microsoft active directory • Identity management • Novell eDirectory • Novell storage services • Novell NetWare platform.	
Unauthorised use	Access that has not been authorised including use which is inappropriate, unlawful and/or criminal (refer to Use of ICT services, facilities and devices policy (IS38) for further clarification).	Queensland Government Glossary for government

7. Document approval details

Document custodian

Director Health Informatics Services, Strategy, Architecture and Information Services Branch, eHealth Queensland

Approval officer

Executive Director, Strategy, Architecture and Information Services Branch, eHealth Queensland

Approval date: 13 April 2023

Version control

Version	Date	Comments
1.0	March 2021	*New guideline*
1.1	April 2023	*Minor amendments (updated references to legislation, standards and policies and business name changes as a result of the Department of Health's Business Case for Change).* *Approved by the Executive Director, Strategy, Architecture and Information Services Branch, eHealth Queensland*

8. Appendix A: Access to applications using Online IT support

8.1. Request access via ServiceNow (SNOW)

To request access to a Queensland Health application, select the Online IT Support portal link (Figure 1), which is available on the Queensland Health Electronic Publishing System (QHEPS).

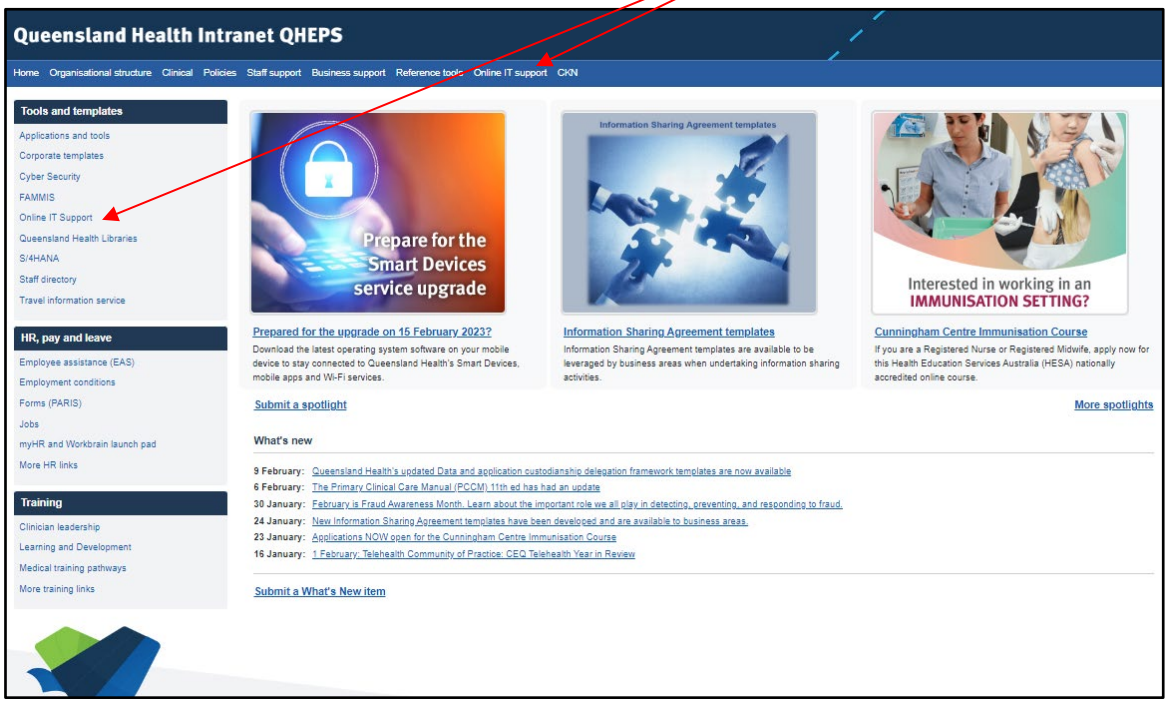

Figure 1 Online IT Support portal

A link to the Online IT Support portal is also available on Queensland Health staff computer desktops (Figure 2).

Figure 2 Desktop Online IT Support link

After selecting the **Online IT Support** portal link, you will be taken to a page in ServiceNow which will display the following options. Select 'Request Access'.

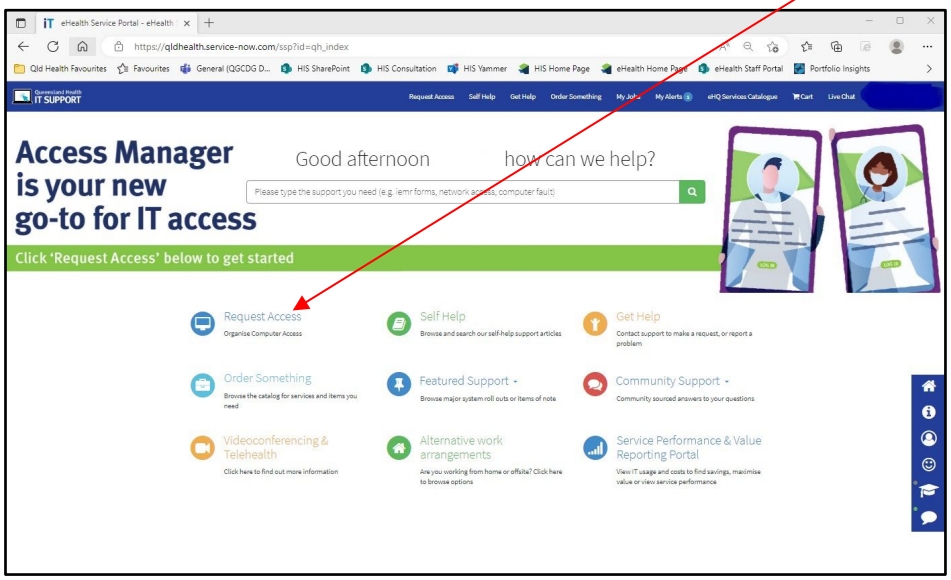

Figure 3 Select 'Request Access'

The following page will appear which includes a list of 'Categories'. Select the 'Applications and Software' category and the drop-down menu will display a number of Queensland Health applications and software. Note: If the application or software is not listed, follow the process set out in sections 8.2 - Access Manager (if your site has Access Manager available) or 8.3 - Online Provisioning System.

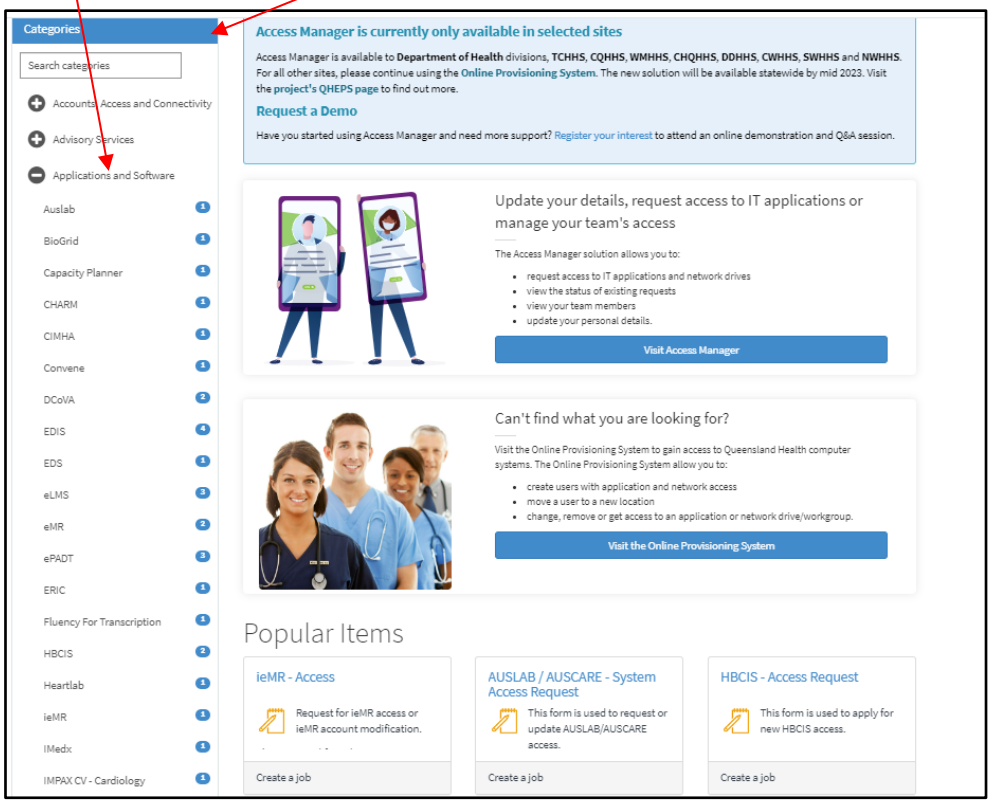

Figure 4 Categories – Application and Software

Select the application from the drop-down menu, for example ieMR, and follow the prompts as detailed in Figure 5.

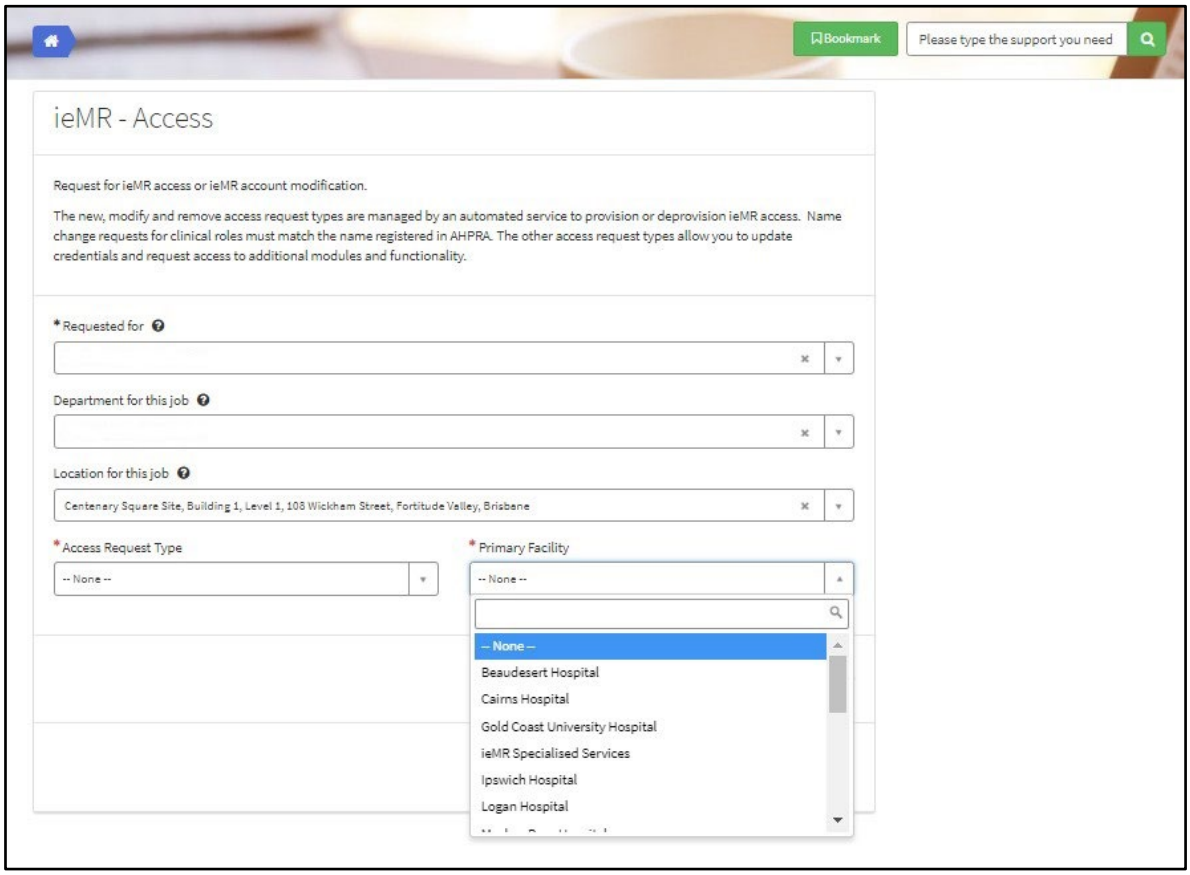

Figure 5 ieMR - Access request

8.2. Access Manager

If the application or software is not listed in SNOW (as per section 8.1), and your site has Access Manager available. use **Access Manager** to request access**.** Sites that currently do not have Access Manager are to continue using the Online Provisioning System (Refer to section 8.3).

Access Manager is an identity and access management solution that provides an efficient and secure process for managing IT access. The appropriate IT access is assigned to the position of an employee rather than an individual. Where an employee commences, moves positions, or leaves the organisation, their IT access will automatically reflect the movements. For example, when an employee moves to a new position, Access Manager will update automatically removing access from the previous position and assigns access requirements of the new position.

Use the Access Manager portal to:

- Request access to IT applications and network drives
- View the status of existing requests
- View team members

- Update personal details.

To open Access Manager, select the Online IT Support portal link. Users will be taken to a page in ServiceNow which will display several options. Select ‘Request Access’.

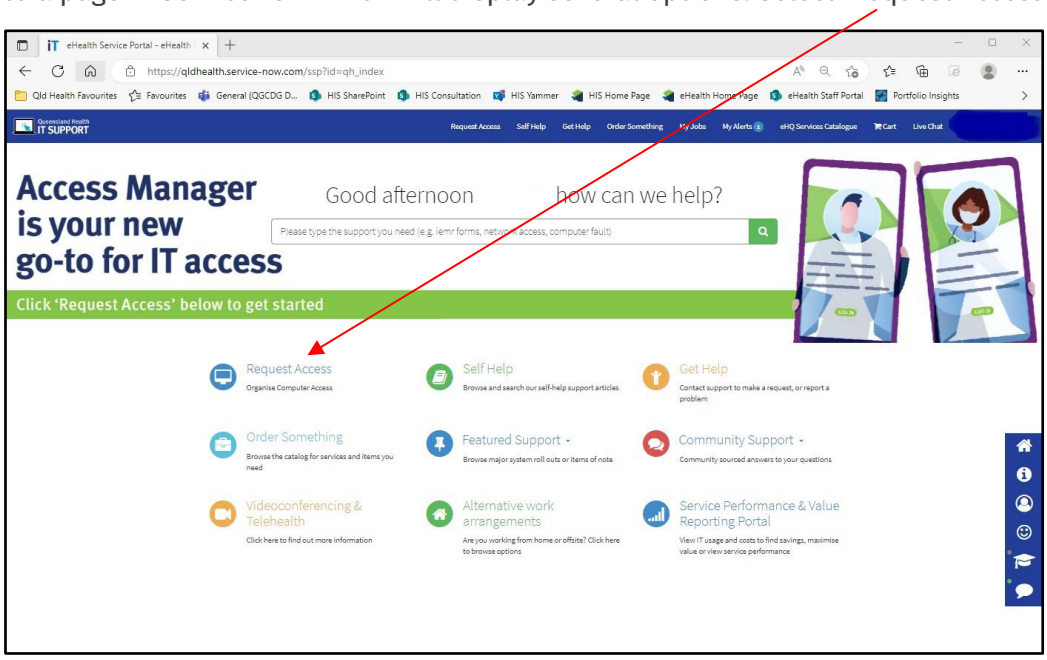

Figure 6 Request Access – Access Manager

The following page will appear. To Open the Access Manager portal, select the ‘Visit Access Manager’ banner.

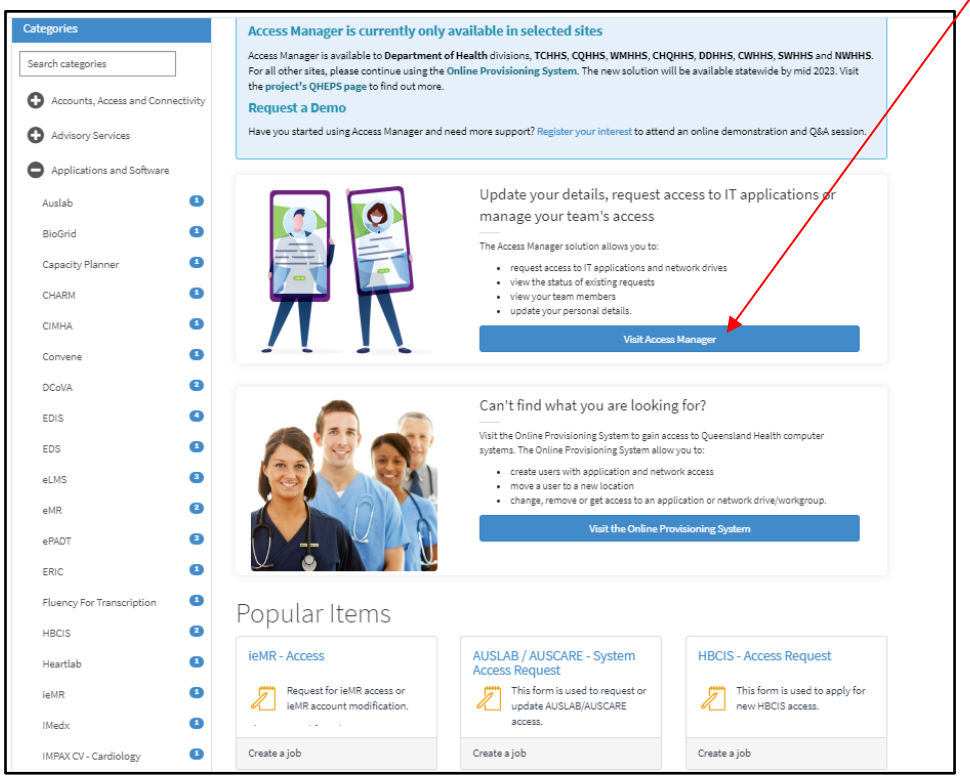

Figure 7 Visit Access Manager

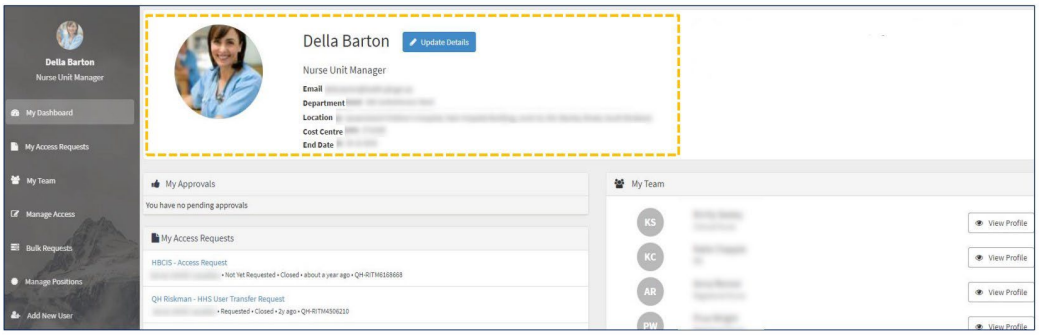

Figure 8 Example Access Manager profile

After selecting the Access Manager banner, the user's personal profile will appear (Figure 8). Personal details and the existing access will be visible in the profile. Staff will be able to edit personal details and manage IT access from this page.

Resources are available to assist users navigate the Access Manager application on the Access Manager QHEPS site.

8.3. Online Provision System

The Online Provisioning System provides a single portal to electronically provision access to Queensland Health applications. The Access Manager application will replace the Online Provisioning System, which will eventually be decommissioned.

The Online Provisioning System is used to:

- Create new network accounts and email accounts for new starters
- Move accounts when users change locations
- Request access to network folders and applications online
- Manage access for employees leaving or changing roles, and
- Manage owned workgroups.

After selecting the **Online IT Support** portal link, you will be taken to a page which will display the following options. Select 'Request Access'.

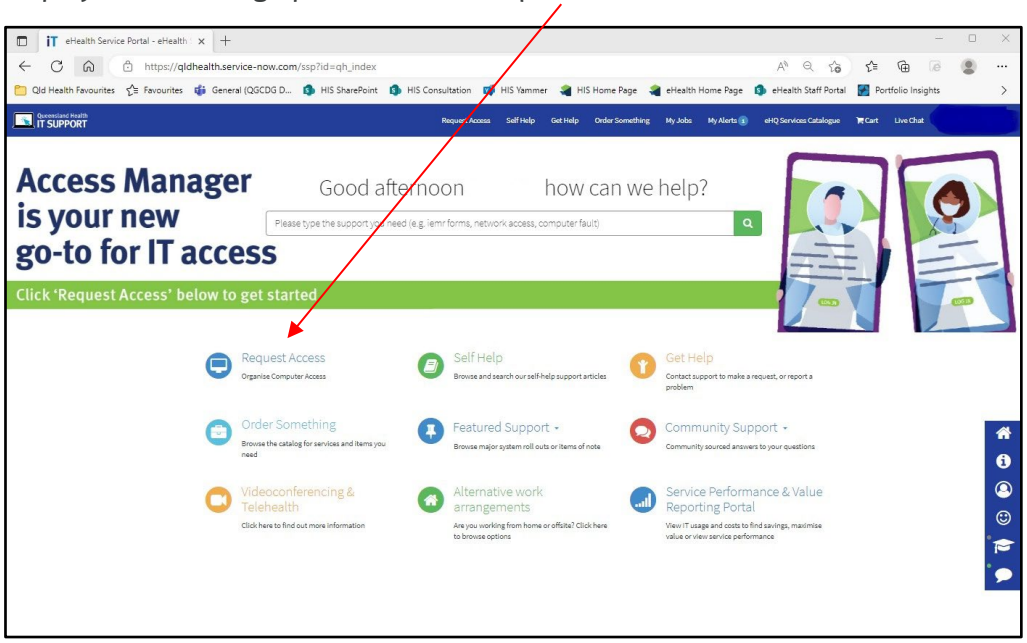

Figure 9 Request Access – Online Provisioning System

The following page will appear. To open the Online Provisioning System portal, select the 'Visit the Online Provisioning System' banner.

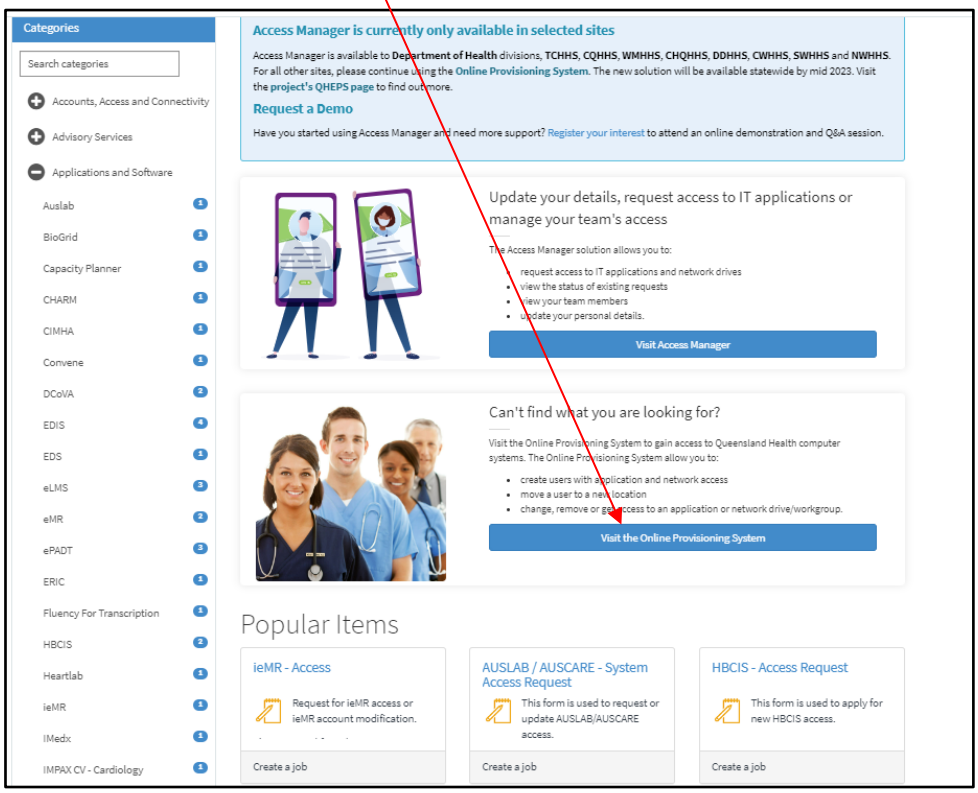

Figure 10 Visit the Online Provisioning System

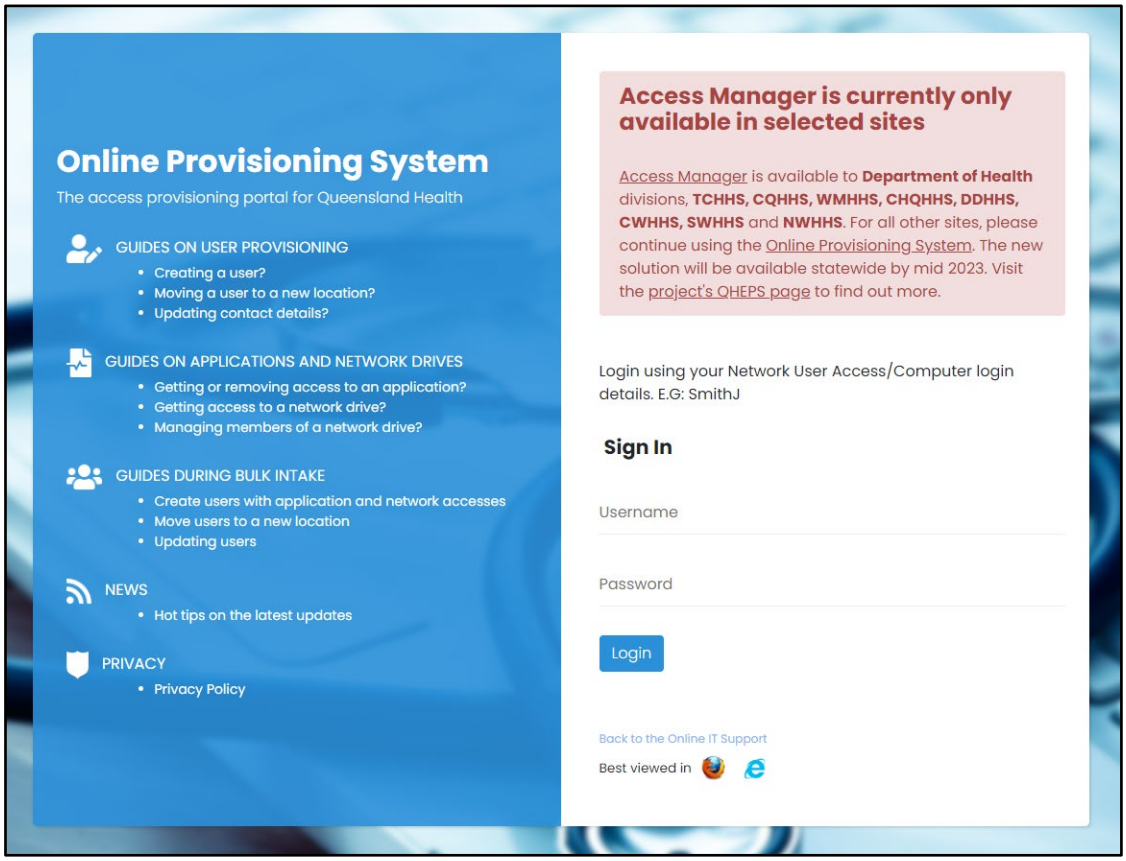

Figure 11 Online Provisioning System Sign in

After selecting the 'Visit the Online Provisioning System' banner, the Sign in prompt will appear (Figure 11).

Upon signing in, the **Main Menu** screen displays all the available options for users to select from (Figure 12).

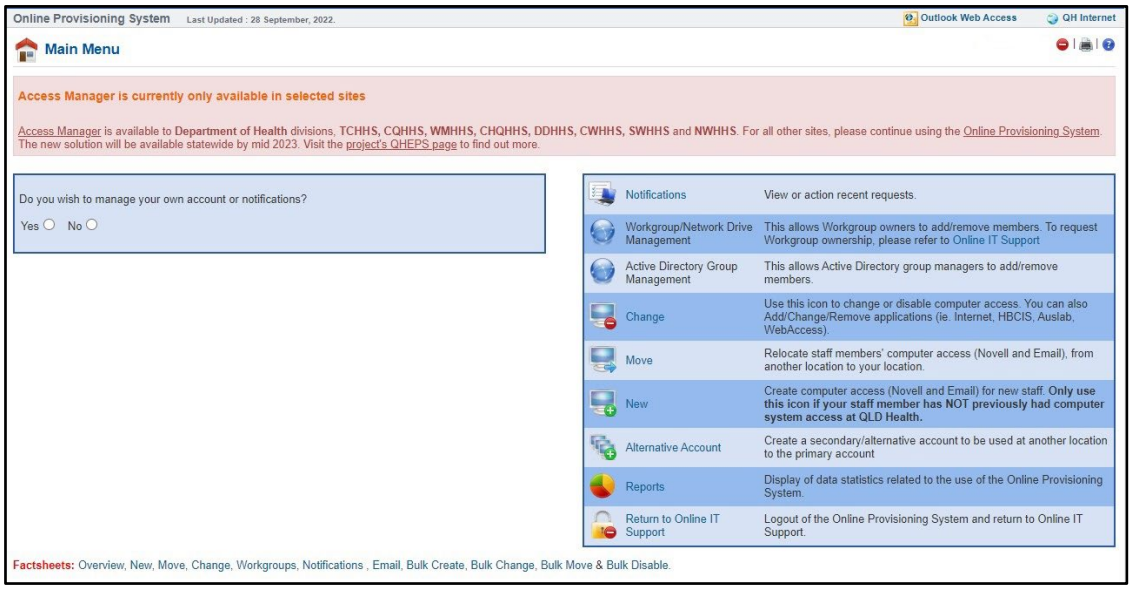

Figure 12 Online Provisioning System Main Menu

For sites that do not have Access Manager, use the Online Provisioning System portal to create a Novell network account, internet access, Outlook account, network drive access and any further applications required for the employees to perform their role. It should be noted that new user account creations are typically performed on behalf of someone else e.g., Authorising line manager. Users requesting access will be required to enter their Novell ID and password to login to the Online Provisioning System.

There are a number of guides available to assist users navigate the Online Provisioning System, including a New Access Factsheet to request an account for new Queensland Health employees.

All authorised users that are granted access to information systems have an obligation to ensure they only access information that is reasonably required for and consistent with the performance of their role and as approved by their line manager or supervisor.

Use the Online Provisioning System portal to change/update user access and select the **Change** option (Figure 9). The **Change** option is used to:

- Change/update a user's account details
- Add additional network drive access
- Add/remove additional applications
- Extend/remove finish date
- Reactivate/terminate access.

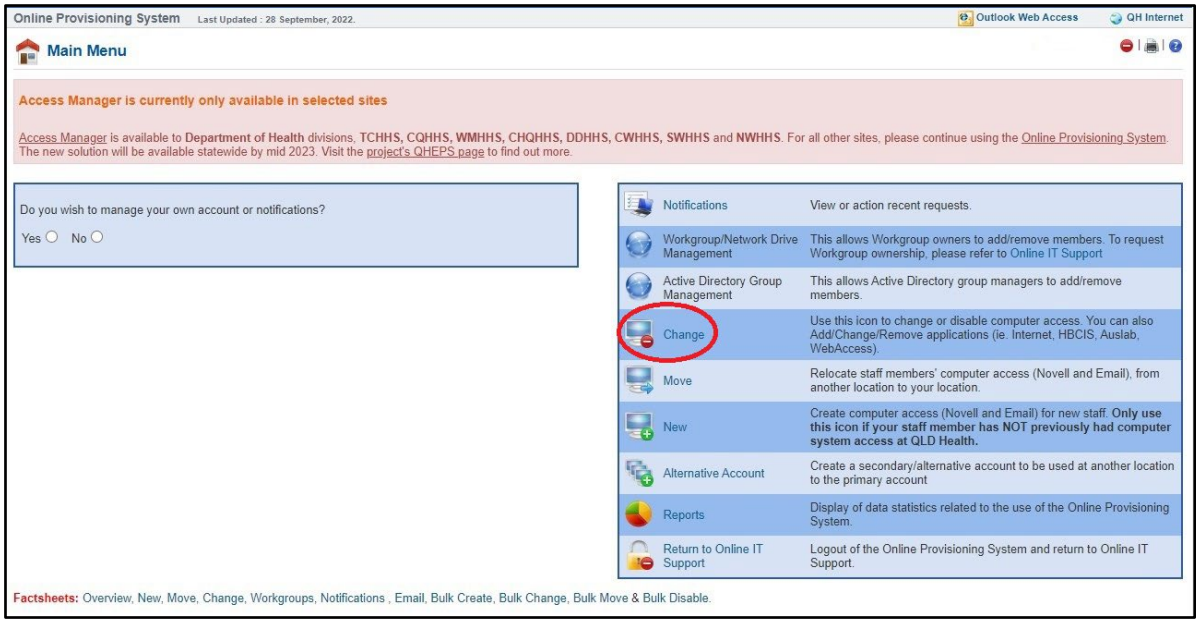

Figure 13 Online Provisioning System - Change

For more information on using the Change option to request changes/updates to user access, refer to the Change Access Factsheet.

9. Appendix B: Example User access review template

Access review form

Privacy Notice
Personal information collected by the Department of Health is handled in accordance with the *Information Privacy Act 2009*. The Department of Health is collecting the information on this <insert name of form> to assist in determining if the request complies with the management of system access security and monitoring controls to ensure personal information is only accessed by authorised persons. The form supports the Data and Application Custodian for <insert application> in authorising system access. The personal information provided by you will be securely stored and only accessible by appropriately authorised officers of the Department of Health. Personal information recorded on this form will not be disclosed to other third parties without consent, unless the disclosure is authorised or required by, or under law. For information about how the Department of Health protects your personal information, or to learn about your right to access your own personal information, please see our website at www.health.qld.gov.au.

9.1. Purpose

The intent of this form is to undertake a user account and access review to determine the access rights and privileges assigned to an application are consistent with business objectives and security principles. The review is to ensure:

- each user access account and the privileges assigned to that account are appropriate and relevant to that user's current role or function.
- that granted access rights and privileges match those documented in an approved access request form.
- the application and the information processed by the application is only accessed and used by authorised users for legitimate reasons.
- users who have left Queensland Health or have changed roles are identified and access is immediately revoked or amended.

This form is to be completed by the user, approved and returned to [add Application Custodian/ Correct delegate details] by [add date to be returned].

9.2. Section A

Applicant details	
Novell ID	
Full name	
Position Title	
Branch/Department/HHS	
Email Address	
Phone Number	

Access details		
Reason access granted *Provide details regarding the reason why you require <type of access (i.e., statewide or HHS/Division)> access to the [name of the application]*	1. Is access required for your current role?	
	2. What type of access is required?	
	3. How often do you use the application?	
Period of Access Required *Access will be removed after 90 days of inactivity.* *Access will be monitored and audited regularly to check that the access to and use of the application is still required for the performance of the employee role.* *Access must never be shared with another employee.*	Start date:	End date:
Applicant Signature:		Date:

9.3. Section B

Supervisor authorisation	
Name:	
Position:	
Department:	
email address:	
Phone:	
Comments:	

I hereby confirm that the access requested is appropriate for the role the applicant is performing. I am satisfied that any segregation of duties conflicts are manageable and where required, compensating controls are introduced. I acknowledge and understand the access which I am authorising for this user.	
Signature:	Date:

9.4. Section C

Administrator Use Only	
Application Custodian or Correct delegate	
Authorisation must be provided prior to retaining/modifying/revoking of a user account. The correct delegate must be a senior officer with a suitable level of authority to endorse this application access request.	
Name:	
Position:	
Department:	
email address:	
Phone:	
Recommended action:	☐ Retain ☐ Modify ☐ Revoke
Comments:	

I hereby give authorisation for retaining/modifying/revoking (strike out options which do not apply) of user access for the applicant.	
Signature:	Date: