Government of **Western Australia**
Department of **Health**

Datix CIMS/CFM Information Access, Use, Disclosure and Disposal Model

Version 2.0 (July 2021)

health.wa.gov.au

Document control

Version	Date	Comment
1.0	December 2016	Original published version
1.1	17 May 2021	Redrafted to align with updated Information Management Policy Framework
1.2	24 May 2021	Draft reviewed by Custodian, comments incorporated
1.3	10 June 2021	Revised draft reviewed by Custodian, comments incorporated
1.4	17 June 2021	Draft reviewed by PSP
1.5	24 June 2021	Final editorial updates; forwarded to Steward for approval
2.0	01 July 2021	Revised version published

Contents

1. Background 2
   1.1 Clinical incident and complaints management in the WA health system 2
   1.2 Datix CIMS/CFM 2
   1.3 Purpose of this document 2
2. Datix CIMS/CFM roles and responsibilities 3
   2.1 Datix CIMS/CFM Steward 3
   2.2 Datix CIMS/CFM Custodians 4
   2.3 Datix CIMS/CFM Administrator 5
   2.4 Datix CIMS/CFM Users 5
3. Access to Datix CIMS/CFM 6
   3.1 Datix CIMS/CFM security profiles 6
   3.2 Requesting a different level access to the Datix CIMS/CFM 9
4. Access, Use and Disclosure of Datix CIMS/CFM data 10
   4.1 Access via WA health system data warehouses 10
   4.2 Regular provision of data to external parties 10
   4.3 Ad hoc requests and data request process 10
   4.4 Releasing Datix CIMS/CFM data 13
   4.5 Datix CIMS/CFM information breaches 13
5. Retention and disposal of Datix CIMS/CFM information 15
6. Glossary 16
Appendix 1 – Datix CIMS/CFM State-wide Access Contract 19
Appendix 2 – Datix CIMS/CFM Data Request Form 20
Appendix 3 – Datix CIMS/CFM Data Release Contract 22
Appendix 4 – Datix CIMS/CFM Data Release Form 23

1. Background

1.1 Clinical incident and complaints management in the WA health system

Clinical incident management and complaints management are two key elements of clinical governance in the Western Australian health system, and the requirements for these processes are set out in mandatory policies issued by the WA Department of Health (Department).

The Clinical Incident Management Policy[1] (CIM Policy) aims to improve patient safety by promoting best practices in CIM to:

- Identify when patients are harmed and implement strategies to minimise harm
- Ensure lessons are learned, provide opportunities to share lessons, and take action to reduce the risk of similar events occurring
- Identify hazards before they cause patient harm, treat the hazard and review clinical risks.

The Complaints Management Policy[2] sets out the requirements for the collection, recording, reporting and management of consumer complaints relating to the WA health system, and promotes best practice in complaints management by advocating an efficient, proactive approach that results in the best possible outcomes for health consumers.

1.2 Datix CIMS/CFM

The Datix Clinical Incident Management System (CIMS) and Consumer Feedback Module (CFM) is an online system used by the WA public health system to efficiently and effectively report and manage clinical incidents and consumer feedback events (including complaints). The Datix CIMS has been used by the WA public health system since February 2014 and the Datix CFM since January 2015. Use of the Datix CIMS/CFM by the WA public health system is mandated by the CIM and Complaints Management Policies respectively.

1.3 Purpose of this document

The purpose of this Datix CIMS/CFM Information Access, Use, Disclosure and Disposal Model is to:

- Explain to users their roles and responsibilities when accessing, using or disclosing information from the Datix CIMS/CFM
- Outline the process for requesting access to the Datix CIMS/CFM and its data
- Assist compliance with the Department's Information Management Policy Framework when accessing, using or disclosing information from the Datix CIMS/CFM.

The Department's Information Access, Use and Disclosure Policy[3] exists to inform employees within the WA health system about how to use and disclose information in a manner that is lawful, and should be read in conjunction with this document.

For further information about this document, the Datix CIMS/CFM, and the CIM and Complaints Management Policies, please contact the Department's Patient Safety Surveillance Unit (PSSU) via email: PSSU@health.wa.gov.au.

[1] The Clinical Incident Management Policy is available at: https://ww2.health.wa.gov.au/About-us/Policy-frameworks/Clinical-Governance-Safety-and-Quality/Mandatory-requirements/Clinical-Incident-Management-Policy
[2] The Complaints Management Policy is available at: https://ww2.health.wa.gov.au/About-us/Policy-frameworks/Clinical-Governance-Safety-and-Quality/Mandatory-requirements/Complaints-Management-Policy
[3] The Information Access, Use and Disclosure Policy is available at: https://ww2.health.wa.gov.au/About-us/Policy-frameworks/Information-Management/Mandatory-requirements/Access-Use-and-Disclosure/Information-Access-Use-and-Disclosure-Policy

2. Datix CIMS/CFM roles and responsibilities

The Datix CIMS/CFM is classified as a Systemwide Information Asset under the Department's Information Management Governance Policy and Model.[4] Overarching responsibility for access, permissions, strategic direction and use of the Datix CIMS/CFM and the information it holds lies with the Steward and Custodians.

The Steward and Custodians are responsible for approving access to the Datix CIMS/CFM and the information it holds and taking reasonable steps to ensure that people with access to the system and its information understand their responsibilities and conditions of access. However, people who are provided with access to the Datix CIMS/CFM and its information are responsible for ensuring that they only access, use and disclose the information for the purposes authorised by the Steward and/or Custodians. The Steward and Custodians are not responsible for how Datix CIMS/CFM data is analysed, used or when it is disseminated further from trusted users including from the WA health system's data warehouses.

2.1 Datix CIMS/CFM Steward

The Steward for the Datix CIMS/CFM is the Assistant Director General Purchasing and System Performance, Department of Health. The Steward is accountable to the Owner (Director General, Department of Health).

The Steward's role is to:

- implement the strategic direction of information management governance that has been recommended by the Information Management Governance Advisory Group and/or approved by the Owner
- manage the Datix CIMS/CFM to ensure compliance in line with legislation, polices and standards.

The Steward's responsibilities include:

- Implement and support the Information Management Governance Model
- Support and provide leadership to the management of the Datix CIMS/CFM
- Provide support to the Custodians on the management of information management practices
- Support information sharing that promotes the access, use and disclosure of information when it is permitted or required by law
- Assign functions to the Custodians and Administrators, and ensure these functions are detailed within the associated Instrument of Delegation and the WA health system Information Register
- Ensure policies under the relevant Policy Frameworks are supported and implemented
- Support participation in the information management communications and education programs
- Review and manage all risks and issues relating to the Datix CIMS/CFM that arise
- Escalate to the Information Management Governance Advisory Group as required
- Ensure physical and technical controls are reviewed, maintained and improved
- Ensure continual improvement to the Datix CIMS/CFM such as quality of information, security, metadata and record management.

[4] The Information Management Governance Policy and Model are available at: https://ww2.health.wa.gov.au/About-us/Policy-frameworks/Information-Management/Mandatory-requirements/Governance/Information-Management-Governance-Policy

2.2 Datix CIMS/CFM Custodians

The Information Management Governance Policy requires Systemwide Information Assets to have both a Systemwide Custodian and, at a minimum, a Custodian at each Health Service Provider (HSP) where the Information Asset is employed. All Custodians are expected to contribute to decisions about Datix CIMS/CFM and are collectively accountable to the Steward.

The Systemwide Custodian for the Datix CIMS/CFM is the Manager PSSU, Department of Health. HSP Custodians are listed in the WA health system Information Register.[5]

Custodians' role is:

- to manage day-to-day operations of the Datix CIMS/CFM, and implement policy on behalf of the Steward
- to grant access to, use and disclosure information from the Datix CIMS/CFM in line with legislation, policy as per delegated authority and in accordance with the Steward's requirements
- to maintain appropriate metadata documentation that is fit-for-purpose
- plan and project manage changes to the Datix CIMS/CFM.

Custodians' responsibilities include:

- Manage the Datix CIMS/CFM in line with policy, relevant legislation and other written laws
- Support information sharing that promotes the access, use and disclosure of information when it is permitted or required by law
- Provide advice on the proper use and interpretation of the information to authorised users
- Ensure the Custodian and Datix CIMS/CFM details are current and accurate within the associated Instruments of Delegation and the WA health system Information Register
- Support and implement relevant policies, processes and procedures
- Participation in all information management communication and education programs
- Maintain a work plan for the Datix CIMS/CFM highlighting risk and mitigation strategies
- Highlight risks and associated mitigation strategies to the Steward
- Escalate risks associated with access, use and disclosure of information to the Steward
- Report and manage information breaches in a timely manner as outlined within relevant policies
- Control access to the Datix CIMS/CFM including regular reviews of users
- Ensure the safe transmission of information to authorised users
- Maintain the security of the Datix CIMS/CFM to ensure privacy and confidentiality of information contained within
- Maintain the quality of the data within the Datix CIMS/CFM including accuracy, completeness, relevance, timeliness, reliability, integrity and consistency to the business needs of the WA health system
- Maintain documentation of metadata, data dictionary and any technical documentation required by policies, legislation or other written laws
- Ensure the record management (retention, storage and disposal) of information is in accordance with policies, legislation and other written laws
- Must participate (or nominate a suitable person to participate) in the State Datix Committee (SDC) and may participate in local Datix CIMS/CFM Business User Groups.

[5] The WA health system Information Register is available to staff in the WA public health system at: https://doh-healthpoint.hdwa.health.wa.gov.au/directory/Purchasing%20and%20System%20Performance/Data%20and%20information/Lists/WA%20health%20system%20Information%20Register/AllItems.aspx

2.3 Datix CIMS/CFM Administrator

The CIMS Support Team at Health Support Services (HSS) is the Administrator for the Datix CIMS/CFM. The role of the HSS CIMS Support Team is to implement rules on behalf of the Custodians and provide technical and administrative support for the Datix CIMS/CFM.

The Administrator's responsibilities include:

- Provide support and technical expertise to Custodians in managing the Datix CIMS/CFM
- Support the Custodians in implementing technical directions to the Datix CIMS/CFM
- Ensure Administrator details are current within the associated Instruments of Delegation and the WA health system Information Register
- Assist the Custodians in the technical implementation of the relevant policies, processes and procedures
- Highlight risks to and within the Datix CIMS/CFM and associated mitigation strategies to the Custodians
- Report and manage information breaches in a timely manner as outlined within policies
- Ensure all physical and technical controls have been applied to the Datix CIMS/CFM
- Assist the Custodians in implementing quality, security, metadata and record management improvements
- May participate in Business User Groups.

2.4 Datix CIMS/CFM Users

Users are individuals or groups that have been provided with access to the Datix CIMS/CFM and/or information either contained in or disclosed from the Datix CIMS/CFM. For clarity, this includes people external to the WA health system that have been provided with information or data obtained from the Datix CIMS/CFM.

The role of Users is to appropriately and lawfully access, use or disclose information contained in the Datix CIMS/CFM as authorised by the Custodians or Steward. Information received or accessed through the Datix CIMS/CFM must only be used for the purpose for which it was approved. Information obtained from the Datix CIMS/CFM must not, under any circumstance, be used in publications or presentations without prior approval in accordance with this Information Access, Use, Disclosure and Disposal Model.

Users' responsibilities include:

- Maintain compliance with the approved usage of information provided by the Custodians
- Comply with the access, use and disclosure contracts, agreements, process or procedures outlined by the Custodians
- Report any suspected breach of information in a timely manner
- Ensure all physical and technical controls are being utilised such as passwords, multi-factor authentication and separation of duties
- Report information quality, functionality or security concerns to the Custodian.

Users who are staff members in the WA health system are also responsible for:

- Complying with the relevant policies within the Policy Frameworks, local policies, processes and procedures
- Participating in all information management communication and education programs relating to the Datix CIMS/CFM.

3. Access to Datix CIMS/CFM

Access to the Datix CIMS/CFM is controlled by a set of location and role-based security profiles that provide users with appropriate permissions within the system. All staff employed within the WA public health system (i.e. that have an HE number) are automatically assigned the **Notifier** security profile (see below). The process for users to request assignment of a different security profile depends on the profile concerned and is described in section 3.2.

3.1 Datix CIMS/CFM security profiles

A summary of the security profiles for Datix CIMS/CFM is presented below. Further information about these security profiles is contained in the Datix CIMS/CFM User Administration and Profiles Guide.[6]

Notifier

The Notifier security profile allows staff members to notify clinical incidents and consumer feedback into the Datix CIMS/CFM.[7] It also provides staff members with read-only access to view clinical incident and consumer feedback records that they have notified.

There is no need for users to request Notifier access to the Datix CIMS/CFM as this is the base profile automatically provided when the HSS CIMS Support Team synchronises the system with the WA health system Active Directory.

Senior Staff

The Senior Staff security profile is usually provided to managers who are responsible for the investigation of clinical incidents and consumer feedback within their area or responsibility.

This security profile provides:

- Read/write access to Datix CIMS records (except for the Head of Department screen which is read only) and Recommendations both at their location and when assigned to them
- Read/write access to Datix CFM records both at their location and when assigned to them as Investigator or invited as a Third Party
- Access to Dashboards, To Do Lists and reporting
- Read only access to the Contacts module.

Senior Staff – CIMS

The Senior Staff – CIMS security profile is also provided to managers who are responsible for the investigation of clinical incidents and consumer feedback within their area or responsibility.

The difference between this profile and the Senior Staff security profile is that it provides **read only** access to Datix CFM records at their location and read/write access when assigned to them as Investigator or Third Party.

Consumer Feedback Coordinator

The Consumer Feedback Coordinator security profile is usually provided to staff members who coordinate the management of consumer feedback, such Customer Service Unit staff and patient/client liaison officers.

---

[6] The Datix CIMS/CFM User Administration and Profiles Guide is available to staff employed in the WA public health system at: https://wahealthdept.sharepoint.com/sites/hss-customer-ict-hosp-admin/SitePages/cims.aspx

[7] Prior to 1 July 2021 the Notifier security profile did not permit access to the Datix CFM (access to notify consumer feedback into Datix CFM was provided via a separate Consumer Feedback Notifier security profile)

This security profile provides:

- Read/write access to all Datix CFM records within their area of responsibility and Recommendations both at their location and when assigned to them
- Read only access to Datix CIMS records at their location
- Access to Dashboards, To Do Lists and reporting
- Read only access to the Contacts module.

Consumer Feedback Investigator

The Consumer Feedback Investigator security profile is usually provided to senior staff/ managers who are responsible for the investigation of consumer feedback.

This security profile provides:

- Read/write access to Datix CFM records where they have been requested to participate in the investigation
- Read only access to other Datix CFM records within their area of responsibility
- Read only access to Datix CIMS records that they have notified
- Access to Dashboards, To Do Lists and reporting.

Head of Department

The Head of Department security profile is usually provided to Directors and Heads of Department who are responsible for endorsing the recommendations resulting from clinical incident investigations or consumer feedback.

This security profile provides:

- Read/write access to Datix CIMS records and Recommendations both at their location and when assigned to them
- Read/write access to Datix CFM records both at their location and when assigned to them as Investigator or invited as a Third Party
- Access to Dashboards, To Do Lists and reporting
- Read only access to the Contacts module.

Third Party

The Third Party security profile may be assigned to any staff member in the WA public health system and allows them to provide input into clinical incident and consumer feedback records that they have been invited to.

This security profile provides:

- Read/write access to the Third party comment, Documentation and Communication & Feedback screens of Datix CIMS records that they have been invited to review
- Read only access to the remaining parts of Datix CIMS records that they have been invited to review
- Read only access to Datix CIMS records that they have notified
- Read/write access to Datix CFM records that they have been invited to review
- Access to Recommendations that are assigned to them
- Access to Dashboards, To Do Lists and reporting for the Datix CIMS/CFM records they have been invited to review.

Safety, Quality & Performance/Clinical Governance Unit (SQP/CGU)

The SQP/CGU security profile is usually provided to Safety, Quality & Performance (SQP) or Clinical Governance Unit (CGU) staff and gives them access to all clinical incidents and consumer feedback within their area of responsibility.

This security profile provides:

- Read/write access to Datix CIMS records and Recommendations both at their location and when assigned to them
- Read/write access to Datix CFM records both at their location and when assigned to them
- Access to Dashboards, To Do Lists and reporting
- Read only access to the Contacts module.

User Admin/SQP

The User Admin/SQP security profile is usually provided to SQP/CGU staff members that have an oversight role for their site, region or HSP to allow them to assign and amend the security profile assigned to staff members in that site, region or HSP.

This security profile provides the same access to Datix CIMS/CFM records as the SQP/CGU profile, with the addition of access to the Administration module, which includes:

- The user lists and the ability to assign and amend user profiles
- Reports administration and the ability to create, manage and share statistical reports with other users.

Users assigned the User Admin/SQP profile must familiarise themselves with, and follow, the instructions contained in the Datix CIMS/CFM User Administration and Profiles Guide.[6]

Health Service Provider Custodians must ensure that the User Admin/SQP profile is restricted to the minimum number of staff members required to allow efficient management of Datix CIMS/CFM user profiles within the HSP. This includes the removal of the User Admin/SQP profile from users that no longer require access to the Administration module.

State-wide access profiles

Security profiles exist that permit access to all records in the Datix CIMS/CFM. These profiles are restricted to staff in the PSSU.

Other state-wide security access profiles exist that permit access to all records in the Datix CIMS. These profiles are restricted to staff in the WA health system holding state-wide portfolios and approved external state government staff to enable them to access relevant state-wide clinical incident details. Access to Datix CIMS for external state government staff is undertaken via a memorandum of understanding (MOU) between the Owner and the Chief Executive (or equivalent) of the agency concerned.

All users with state-wide access to the Datix CIMS/CFM that intend extracting data and/or preparing reports for release to third parties must first submit a data request for approval by the Systemwide Custodian. Additionally, the resultant data extract and/or report requires the review and approval of the Systemwide Custodian prior to release to any third party.

System Administrator

The System Administrator security profile provides full system administration access and is restricted to the HSS CIMS Support Team.

3.2 Requesting a different level access to the Datix CIMS/CFM

The process for WA health system users to request a different security profile to **Notifier** depends on the profile concerned. All requests require completion of one of the Datix CIMS/CFM User Access Request Forms available on the HSS CIMS intranet page.[8] Users requiring higher-level access for more than one site (e.g. staff that work in two hospitals in different HSPs) will need to complete multiple forms.

All security profiles other than User Admin/SQP, System Administrator and state-wide access profiles

All requests for security profiles other than User Admin/SQP, System Administrator and state-wide access profiles are handled via local processes. Local processes may vary slightly between HSPs, however the basic the steps are:

- The user completes the Datix CIMS/CFM User Access Request Form indicating the security profile they are requesting and emails the form to the delegated authority within their HSP for approval
- The delegated authority completes the approval section of the form, and if approved emails the form to the site/region/HSP User Administrator
- The User Administrator amends the user's security profile and informs the user. The User Administrator is responsible for ensuring the request form has been completed accurately and is saved in an appropriate location, as the form will need to be produced in the event of a profile/security audit.

User Admin/SQP

Requests for User Admin/SQP access require local approval prior to processing by the HSS CIMS Support Team. The steps are:

- The user completes the Datix CIMS/CFM User Administrator Form and emails the form to the delegated authority within their HSP for approval
- The delegated authority completes the approval section of the form, and if approved emails the form to the HSS CIMS Support Team
- The HSS CIMS Support Team amends the user's security profile and informs the user. The HSS CIMS Support Team is responsible for ensuring the request form has been completed accurately and is saved in an appropriate location.

System Administrator and state-wide access profiles

Requests for System Administrator and state-wide access security profiles must be approved by the Systemwide Custodian prior to processing by the HSS CIMS Support Team. The steps are:

- The user completes the Datix CIMS/CFM State-wide Access Form[9] indicating the security profile they are requesting and the Datix CIMS/CFM State-wide Access Contract (see Appendix 1) then emails both forms to the Systemwide Custodian via PSSU@health.wa.gov.au
- The Systemwide Custodian completes the approval section of the form, and if approved emails the form to the HSS CIMS Support Team
- The HSS CIMS Support Team amends the user's security profile and informs the user. The HSS CIMS Support Team is responsible for ensuring the request form has been completed accurately and is saved in an appropriate location.

[8] The Datix CIMS/CFM User Access Request Forms are available to staff in the WA public health system at: https://wahealthdept.sharepoint.com/sites/hss-customer-ict-hosp-admin/SitePages/cims.aspx

[9] The Datix CIMS/CFM State-wide Access Form is also used to request access to the Datix Rich Client application

4. Access, Use and Disclosure of Datix CIMS/CFM data

There are multiple mechanisms by which access to Datix CIMS/CFM data may be provided, including:

- Via the WA health system's data warehouses
- Regular provision of (or access to) data to external parties
- Ad hoc requests, including requests related to research or made under the *Freedom of Information Act 1992* (FOI Act).

4.1 Access via WA health system data warehouses

The use of business intelligence (BI) tools to collate, analyse and disseminate WA health system data has resulted in the establishment of data warehouses. The WA health system's data warehouses may receive data from multiple enterprise systems including Datix CIMS/CFM.

Requests for Datix CIMS/CFM data to be provided to WA health system data warehouses require approval from the Datix CIMS/CFM Systemwide Custodian and Steward and the data warehouse custodian.

Once BI access is approved and established, the use of Datix CIMS/CFM data from the WA health system's data warehouses or to populate reports and dashboards requires additional approval from both an appropriate Datix CIMS/CFM Custodian (based on the scope of the data) and the data warehouse custodian. If these dashboards or reports will be published outside of the WA public health system (e.g. public reporting) then further approval from the Datix CIMS/CFM Steward may be required. This is to ensure that non-personal data and personal (identifiable) data are approved for release considering the sensitivity and confidentiality of the data, and in accordance with the Department's Information Access, Use and Disclosure Policy.

Dashboards and reports containing Datix CIMS/CFM are prohibited from:

- Using free-text fields (unless the Systemwide Custodian has given permission)
- Displaying any personal information, other than the CIMS/CFM reference numbers relating to the data presented.

4.2 Regular provision of data to external parties

For regular provision of/or access to Datix CIMS/CFM data by third parties external to the WA public health system, a contract or MOU between the Owner and the third party may be required to ensure access to confidential health information is lawful, limited to the agreed use, and that appropriate safeguards are in place to protect information, including on termination of the agreement. The contract or MOU should enable the Department to audit the third party's compliance with the contract/MOU and the Department's information security standards.

A thorough risk assessment will be conducted by the Systemwide Custodian prior to authorising regular provision of/access to Datix CIMS/CFM data by third parties. This may include site visits to third parties to ensure the Department's information security standards are met in the areas of physical and network security and access and administrative controls.

4.3 Ad hoc requests and data request process

Ad hoc requests for access to Datix CIMS/CFM data may be made by staff within the WA health system and third parties external to it (e.g. researchers, universities, external contractors, non-government organisations and state and federal agencies). The nature, scope and intended use of the data will determine the approvals that are required, which may include approval by an appropriate Human Research Ethics Committee (HREC), a Datix CIMS/CFM Custodian, the Datix CIMS/CFM Steward, and hospital or HSP Executive (see Table 1).

Table 1: Approvals required for access and disclosure of Datix CIMS/CFM data

Purpose for which the information is accessed and/or disclosed	**Information Classification***		
	Public Non-personal published aggregated information	**Protected** Non-personal aggregated information and non-patient identifiable record level information	**Confidential** Personal (reasonably identifiable) record level information
Authorised National Reporting Bodies	No restriction	Approval by a Datix CIMS/CFM Custodian	Approval by a Datix CIMS/CFM Custodian
For a legal purpose authorised in the *Health Services Act 2016*	No restriction	Approval by a Datix CIMS/CFM Custodian	Approval by a Datix CIMS/CFM Custodian **AND** the Datix CIMS/ CFM Steward
Responding to a request under the *Freedom of Information Act 1992*	No restriction	Approval by a Datix CIMS/CFM Custodian **AND** a decision maker authorised by the Director General under the FOI Act	Approval by a Datix CIMS/CFM Custodian **AND** a decision maker authorised by the Director General under the FOI Act
For a legal purpose authorised by other written laws (e.g. disclosure under the *Child Protection Act*)	No restriction	In accordance with the applicable legislation, policies and site requirements **AND** approval by a Datix CIMS/CFM Custodian	In accordance with the applicable legislation, policies and site requirements **AND** approval by a Datix CIMS/CFM Custodian
Research	No restriction	Approval by a Datix CIMS/CFM Custodian **AND** the Datix CIMS/ CFM Steward[#] **AND** ethical approval from a WA health system HREC and site research authorisation	Approval by a Datix CIMS/CFM Custodian **AND** the Datix CIMS/ CFM Steward **AND** ethical approval from a WA health system HREC and site research authorisation
Other (e.g. disclosure to answer a ministerial, parliamentary question or in response to other external queries)	No restriction	Approval by a Datix CIMS/CFM Custodian (**AND** a WA health system HREC if required)	Approval by a Datix CIMS/CFM Custodian **AND** the Datix CIMS/ CFM Steward (**AND** a WA health system HREC if required)

* For a more detailed explanation of these terms please refer to the Glossary

[#] Datix CIMS/CFM Steward approval is required where the research is external to the WA public health system

The Datix CIMS/CFM has both a Systemwide Custodian and HSP Custodians, who have different scope to approve access and disclosure of Datix CIMS/CFM information. The Systemwide Custodian may approve the access and disclosure of all Datix CIMS/CFM information, including HSP and hospital/site level information. HSP Custodians have more limited scope, which is set out in the WA health system Information Register.[5]

Requests for access to Datix CIMS/CFM information, other than requests made under the FOI Act, must be submitted to the appropriate Datix CIMS/CFM Custodian using the Datix CIMS/ CFM Data Request Form (see Appendix 2). HSP Custodians that receive Datix CIMS/CFM Data Request Forms that exceed their scope should refer these to the Systemwide Custodian.

Several resources are available to facilitate requestors' understanding of the Datix CIMS/CFM datasets and assist with the submission of data requests. These include the Datix CIMS Data Dictionary, Datix CIMS Incident Classification System, and Datix CFM Issue Categories.[10] Copies of these resources can be provided to requestors external to the WA public health system upon request.

Queries regarding access to Datix CIMS/CFM data (including appropriate Custodians) and completed Data Request Forms for information that exceed the scope of an HSP Custodian should be submitted to the Systemwide Custodian via email to PSSU@health.wa.gov.au. Requests will be considered in accordance with the Information Access, Use and Disclosure Policy on a case-by-case basis.

Requests for Datix CIMS/CFM information under the FOI Act

All requests for access to Datix CIMS/CFM information via the FOI Act must be submitted to an appropriate FOI office/coordinator who will liaise with the relevant Custodians/stakeholders to source information of relevance the request. This is because the FOI Act places statutory requirements on the response to the request, including the timeframe in which the response must be provided.

Requests for state-wide Datix CIMS/CFM information under the FOI Act should be submitted to the Department's FOI Coordinator via email to FOI.DOH@health.wa.gov.au. Completion of the Datix CIMS/CFM Data Request Form is **NOT** required for requests made under the FOI Act. The FOI office/coordinator will release the any information of relevance found to the requestor.

Research-related requests for Datix CIMS/CFM information

Access, use and disclosure of information for research purposes requires specific governance processes which may be specific to local collections, and local policies/procedures/guidelines. One such governance process is the ethical review of research projects. All human research must be ethically and scientifically reviewed through an appropriate pathway by a Human Research Ethics Committee (HREC) as detailed in the Research Governance Procedure.[11]

Research projects that require approval from a WA health system HREC include:

- requests for information by entities external to the WA health system
- research projects involving the use and disclosure of information from information assets held by WA health system
- requests deemed by a Custodian to be sensitive or requiring ethics approval.

[10] These Datix CIMS/CFM resources are available to users in the WA public health system at: https://wahealthdept.sharepoint.com/sites/hss-customer-ict-hosp-admin/SitePages/cims.aspx

[11] The Research Governance Policy and Procedure is available at: https://ww2.health.wa.gov.au/About-us/Policy-frameworks/Research/Mandatory-requirements/Research-Governance-Policy

While researchers are welcome to discuss their project and Datix CIMS/CFM data request with the Systemwide Custodian, ethical approval must be granted by a WA health system HREC before any protected or confidential Datix CIMS/CFM data will be disclosed for research purposes. Evidence of ethical approval for the research (and site authorisation if required) must be submitted in conjunction with the Datix CIMS/CFM Data Request Form.

4.4 Releasing Datix CIMS/CFM data

Prior to releasing data, the Datix CIMS/CFM Data Release Contract (see Appendix 3) must be completed by the requestor. This outlines the obligations of the requestor, limitations on usage of the data (including restrictions on further dissemination of the data to third parties) and how the data will be stored. It allows the Datix CIMS/CFM Custodians to ensure and be confident that the recipient of the data fully understands the conditions of its release and their obligations. This is particularly important when releasing confidential and/or sensitive information.

The Datix CIMS/CFM Data Release Form (see Appendix 4) is to be completed by the person who extracted the information before supplying the data to the requestor. The Data Release Form documents the specifications of the data that has been extracted, including any known issues with data elements and serves as a record for the Custodian/s. A contact who can respond to any enquiries from the requestor and/or recipient is also documented on this form. For recurring data requests, the Data Release Form only needs to be completed for the initial request unless substantial modifications to the data request are made.

Data extracted from the Datix CIMS/CFM will be checked against related data to ensure consistency where possible. Data will not be released from the Datix CIMS/CFM without the necessary approvals in accordance with this Information Access, Use, Disclosure and Disposal Model. Data supplied from the Datix CIMS/CFM through the data request process will have a look and feel common to other WA health system products.

Confidential, sensitive or patient-identifiable data must be transferred to the recipient in a secure manner in accordance with the Department's Information Security Policy.[12] My File eXchange (MyFX) and My File Transfer (MyFT) are services available to HSPs and the Department to allow staff to send and receive health, personal and other confidential or sensitive information safely and securely.

4.5 Datix CIMS/CFM information breaches

In respect of the Datix CIMS/CFM, an information breach occurs when Datix CIMS/CFM information is subject to unauthorised access, use or disclosure, or is lost, damaged or destroyed. An information breach may be caused by malicious action (by an external or insider party), human error, or a failure in information handling or security systems.

Examples of Datix CIMS/CFM information breaches could include:

- Loss or theft of printed copies of incident or complaint records that contain personal information
- A staff member with the User Admin/SQP security profile assigns the incorrect security profile to another user, allowing unauthorised access to Datix CIMS/CFM records
- Inadvertent disclosure of personal information due to 'human error', for example the output of a Datix CIMS/CFM data request is released to the wrong person.

[12] The Information Security Policy is available at: https://ww2.health.wa.gov.au/About-us/Policy-frameworks/Information-and-Communications-Technology/Mandatory-requirements/Information-Security-Policy

Datix CIMS/CFM information breaches must be managed in accordance with the Department's Information Breach Policy[13] to minimise the damage of the information breach, including taking action to contain the information breach, assess the impact of the information breach to determine the extent of the damage and harm caused, remediate any risk of further harm, and review the incident and take preventative actions.

In the event of a Datix CIMS/CFM information breach the person who discovers the breach should immediately initiate a process of containment by taking whatever steps possible to limit any further unauthorised access, loss, damage and/or distribution of the information.

The person who discovers a Datix CIMS/CFM information breach must also:

- Immediately notify the Systemwide Custodian and relevant Integrity Unit
- Promptly gather as much information as possible and complete parts 1 and 2 of the Information Breach Notification Form then forward the completed Information Breach Notification Form to the Systemwide Custodian within 24 hours of discovery.

The Systemwide Custodian will assess the information provided in the Information Breach Notification Form and work with stakeholders including Managers, HSP Custodians and System Administrators to determine the severity and impact of the information breach and whether further action and/or investigation is required. Consideration will also be given to whether the nature of the breach and the information concerned requires any affected individuals to be informed, and whether other entities should be notified (e.g. police/law enforcement, Corruption and Crime Commission (CCC) and other agencies/organisations affected by the breach).

The Director General and HSP Chief Executives have a statutory obligation to report all incidents of suspected misconduct to the CCC. If there has been an intentional or suspected breach of Datix CIMS/CFM information by a staff member in the WA health system, it is important that staff should report this as soon as practicable to the Systemwide Custodian and the relevant Integrity Unit.

The Systemwide Custodian will also work with stakeholders to agree the appropriate actions to be taken to minimise the possibility of a similar breach of Datix CIMS/CFM information occurring in the future and forward the completed Information Breach Notification Form to the Department's Information Governance and Performance Unit.

Requests for Datix CIMS/CFM user data/information

Requests for information about users that may have accessed or modified records in the Datix CIMS/CFM may be made by selected staff in the WA public health system and are subject to HSS's Request for User Data/Information process.[14] Such requests are made by completing the 'Application Audit Request' section of the Request for User Data/Information - Investigation form and submitting it to HSSSecurityAuditRequests@health.wa.gov.au.

Application audit requests require the approval of an appropriate Datix CIMS/CFM Custodian which will be facilitated by HSS. Custodians will consider Datix CIMS/CFM application audit requests on a case-by-case basis. WA public health system staff wishing to make a Datix CIMS/CFM application audit request are strongly encouraged to contact the Systemwide Custodian via PSSU@health.wa.gov.au to discuss if the information sought may be available.

[13] The Information Breach Policy is available at: https://ww2.health.wa.gov.au/About-us/Policy-frameworks/Information-Management/Mandatory-requirements/Access-Use-and-Disclosure/Information-Breach-Policy

[14] Information about the Request for User Data/Information process is available to WA public health system staff at: https://healthpoint.hdwa.health.wa.gov.au/workingathealth/it/Security%20Documents/Request-for-User-Data-Information.doc

5. Retention and disposal of Datix CIMS/CFM information

Digital records held in the Datix CIMS/CFM are required to be retained and disposed of in accordance with the Department's Information Retention and Disposal Policy[15] and its associated disposal authorities and schedules.

The minimum retention period for individual Datix CIMS/CFM records may differ depending on the circumstances of the clinical incident or complaint. Of particular note, in 2020 the WA Government issued the General Retention and Disposal Authority for Incidents and Allegations of Child Abuse or Neglect.[16] This requires that records (including initial allegations, complaints or reports, and investigation or inquiry records) of allegations or incidents of child abuse or neglect concerning a staff member or other person engaged by a WA Government entity must be retained for 100 years before destruction.

The Datix CIMS/CFM Systemwide Custodian and System Administrator are responsible for ensuring that digital records held in the Datix CIMS/CFM remain accessible for the applicable retention period(s), including beyond end-of-life of the Datix CIMS/CFM and monitoring to identify any digital formats that may be at risk of obsolescence. Users should be mindful not to delete records from the Datix CIMS/CFM in contravention of the Information Retention and Disposal Policy.

Users that receive information extracted from the Datix CIMS/CFM in response to a formal data request are permitted to retain the extracted information for the period specified in the data request form. Unless otherwise authorised by the relevant Datix CIMS/CFM Custodian, the user must destroy all copies of the Datix CIMS/CFM information (including any hard copies) upon completion of its use for the purpose intended and inform the Custodian of the outcome.

[15] The Information Retention and Disposal Policy is available at: https://ww2.health.wa.gov.au/About-us/Policy-frameworks/Information-Management/Mandatory-requirements/Storage-and-Disposal/Information-Retention-and-Disposal-Policy

[16] The General Retention and Disposal Authority for Incidents and Allegations of Child Abuse or Neglect is available at: https://www.wa.gov.au/sites/default/files/2021-02/2020-003.pdf

6. Glossary

Term	Meaning
Access	Refers to the right or opportunity to use or view information. An individual enacts this access when they use, view or enter the environment in which this information is held. This includes both direct access to information systems/ databases, and access to information extracted from systems/databases.
Aggregated information	Summed and/or categorised information that is analysed and placed in a format (for example, in tables or graphs) that prevents the chance of revealing an individual's identity (i.e. individual records cannot be reconstructed).
Dashboards	Reports and visualisations created using data from the Datix CIMS/CFM that allow users to view and interact with information in predefined formats, but not to modify data stored within the Datix CIMS/CFM or a data repository.
Data	Refers to unprocessed information, while the term 'information' refers to data that has been processed in such a way as to be meaningful to the person who receives it. The terms 'data' and 'information' are often used interchangeably and should be taken to mean both data and information.
Data Custodian	The person(s) responsible for the day-to-day management of a data collection.
Data Steward	A position with delegated responsibility from the Director General of the Department of Health to manage a data collection.
Data warehouse	Integrates data from various Enterprise and Local systems and stores them in an easily accessible central repository. A data warehouse is designed to support business decisions by facilitating the consolidation of data to support analysis and reporting at different aggregate levels. The integration of query, reporting and analysis tools provides users with the opportunity to efficiently extract critical data as well as drill down and through the data for clinical and operational analytics.
Disclosure	A person discloses information if they cause the information to appear, allow the information to be seen, make the information known, reveal the information or lay the information open to view.
Health information	Has the meaning given in the Health Services Act 2016 in section 213 as: (a) information, or an opinion, that is also personal information, about: (i) the health (at any time) of an individual; or (ii) a disability (at any time) of an individual; or (iii) an individual's expressed wishes about the future provision of health services to the individual; or (iv) a health service provided, or to be provided, to an individual; or (b) other personal information collected to provide, or in providing, a health service.
Human Research Ethics Committee (HREC)	HRECs are responsible for the review and approval of research proposals where research involves humans. HRECs must be constituted in accordance with, and act in compliance with, the *National Statement on Ethical Conduct in Human Research*, as in force from time to time, issued under the *National Health and Medical Research Council Act 1992 (Cth).*

Term	Meaning
Information	Refers to data that has been processed in such a way as to be meaningful to the person who receives it. Information can be personal or non-personal in nature. The terms 'data' and 'information' are often used interchangeably and should be taken to mean both data and information.
Information breach	An incident, in which personal or confidential information, or non-personal information that could be sensitive or commercial, is compromised, disclosed, copied, transmitted, accessed, removed, destroyed, stolen or used by unauthorised individuals, whether accidentally or intentionally.
Information classification	In the context of this Information Access, Use, Disclosure and Disposal Model, three levels of information are described to enable appropriate governance over access and disclosure of Datix CIMS/CFM information: • Public – non-personal aggregated data that has already been publicly released by the WA Department of Health, such as that included in the *Your safety in our hands in hospital* report. While further approval to reference, quote or re-use aggregated Datix CIMS/CFM information that has been publicly released is not required, users doing so must ensure the source of the information is appropriately referenced. • Protected – non-personal aggregated data that has <u>not</u> already been publicly released by the WA Department of Health (e.g. information disclosed in response to a Datix CIMS/CFM data request or that has previously been published within the WA public health system), and all non-patient identifiable record level Datix CIMS/CFM information. • Confidential – personal (reasonably identifiable) record level Datix CIMS/CFM information. Whether Datix CIMS/CFM information is reasonably identifiable or not is dependent on the nature and extent of the information, who the information is available/released to and any other information or datasets that the user/recipient holds or has access to.
Legal purpose	Refers to the purpose that is authorised by the Health Services Act 2016, the Health Services (Information) Regulations 2017 or any other written laws. It does not refer to the operational purpose or an operational fit-for-purpose assessment.
Non-personal information	Information from which a person's identity is not apparent and cannot be reasonably ascertained. Whether information is truly non-personal will depend on the context, including the nature of the information, the number of people to whom it could potentially relate, and the amount of information proposed to be disclosed. Although a series of individual pieces of information may not, on their own, enable the identity of an individual to be ascertained, identification may occur when all the pieces of information are combined.
Operational purpose	Refers to the purpose for which an operational activity, action or procedure is undertaken. It does not refer to the legal purpose for which an activity, action or procedure is undertaken.
Personal information	Has the meaning given in the *Freedom of Information Act 1992*: Means information or an opinion, whether true or not, and whether recorded in a material form or not, about an individual, whether living or dead — (a) whose identity is apparent or can reasonably be ascertained from the information or opinion; or (b) who can be identified by reference to an identification number or other identifying particular such as a fingerprint, retina print or body sample.

Term	Meaning
Reasonably identifiable information	Reasonably identifiable information is personal information. It includes information connected with an individual's name, image, date of birth or address; information that contains a unique personal identifier when the holder of the information also has the master list linking the identifiers to individuals; and information that the holder can merge or link to other information they already hold, enabling them to identify individuals. Whether Datix CIMS/CFM information is reasonably identifiable or not is therefore dependent on the nature and extent of the information, who the information is available/released to and any other information or datasets that the user/recipient holds or has access to.
Record level information	Is usually data at the level of an individual event, person or clinician. Record level data need not directly identify the patient but is more vulnerable to re-identification than aggregate data.
Research	Original investigation undertaken to gain knowledge, understanding and insight as described in the National Health and Medical Research Council's *Australian Code for the Responsible Conduct for Research*. The concept of research is broad and includes the creation of new knowledge and/or the use of existing knowledge in a new and creative way so as to generate new concepts, methodologies, inventions and understandings. This could include synthesis and analysis of previous research to the extent that it is new and creative.
Sensitive information	Refers to information that might result in an adverse impact(s) on an individual, the WA health system, the government and/or other third parties.
Site research authorisation	Before research can commence at a nominated site, the WA health system entity's Research Governance Office must conduct a site review and provide site authorisation. The site review is a comprehensive risk assessment, including verification of ethical approval/s.
Use	A person uses information if they utilise, handle, collect or communicate information within the WA health system or employ information for a purpose.

Appendix 1 – Datix CIMS/CFM State-wide Access Contract

This contract is designed to protect the confidentiality and integrity of health information and patient data contained in the Datix CIMS/CFM

WA health system staff granted state-wide access to the Datix CIMS/CFM are required to adhere to strict obligations

By signing this contract, the user:

- Agrees to maintain Datix CIMS/CFM information in a confidential and secure manner and in the location in which it originally resides.
- Acknowledges that any Datix CIMS/CFM information approved for release remains the property of the WA health system.
- Agrees to, under no circumstances, pass on or divulge Datix CIMS/CFM information to a third party without the prior approval of the relevant Datix CIMS/CFM Custodian.
- Agrees not to use Datix CIMS/CFM information for any purpose other than that for which state-wide access was originally granted.
- Agrees that the source of Datix CIMS/CFM information will be properly referenced whenever it is approved for use in publications.
- Agrees not to copy or store parts or the whole of the Datix CIMS/CFM dataset in a directory or location that may be accessible to anyone else.
- Agrees not to leave printouts of Datix CIMS/CFM datasets in any form in an area accessible to anyone else.
- Agrees to destroy all electronic and hard copies of Datix CIMS/CFM information extracted from the system upon completion of its use for the purpose intended and inform the relevant Datix CIMS/CFM Custodian of the outcome.

DISCLAIMER

All Datix CIMS/CFM information/data is accurate and up to date at the time of access or extraction from the system. The WA health system cannot be held liable for the accuracy of the reports based on the analysis of the data.

CONTRACT

I _____ *(please print)*

of _____ *(department/organisation)*

Acknowledge that I have read and agree to the above provisions of the contract to access and use state-wide Datix CIMS/CFM data.

Signed:			
Position/Title:		Date:	
Witnessed by:		Position:	
Signature:		Date:	

Office Use Only

Reference No:		Received by:	

To request state-wide access to Datix CIMS/CFM, complete this contract and submit with a completed Datix CIMS/CFM State-wide Access Form to the Systemwide Custodian via PSSU@health.wa.gov.au.

Appendix 2 – Datix CIMS/CFM Data Request Form

This form is to be completed for all requests to access Datix CIMS/CFM data, apart from requests made under the *Freedom of Information Act 1992*. The requestor must fully complete Section 1.

SECTION 1: REQUEST DETAILS			
Requestor name:		Phone:	
Position:		Email:	
Work location:			
Ethics No:			
Provide by: *(date)*		Recurrence:	
Project Title:			
Project summary/ purpose:			
Data items/variables required: *(please be specific and indicate CIMS or CFM)* Refer to the Datix CIMS Data Dictionary for information about Datix CIMS variables			
	Description: (*general summary)*		
	Date range of data:		
	Locations/Site:		
	Other in/exclusions:		
How will the data be stored?			
Who will have access to the data?			
How and to who will the data be disseminated/published?			
Data retention period: *(data must be deleted after this date)*		Duration: End date:	
Requestor Signature: *(HE no. if electronic)*		Date:	
Head of Dept Name:		Signature: *(HE no. if electronic)*	
Department/Site:		Date:	

SECTION 2: APPROVAL DETAILS			
Request Number:		Date received:	
Comments:			
Datix CIMS/CFM Custodian Recommendation:	☐ Approved ☐ Not Approved	Signature: *(HE no. if electronic)* Date:	
Data Warehouse Custodian Recommendation:	☐ Approved ☐ Not Approved	Signature: *(HE no. if electronic)* Date:	
Datix CIMS/CFM Steward Approval Status: *(as applicable- to be completed by Data Steward)*	☐ Approved ☐ Not Approved	Signature: Date:	

SECTION 3: COMPLETION DETAILS			
Date Completed:		Date Provided:	
Revisions Required:			
Feedback/Comments:			

Requestors within the WA Public health system should send the completed Datix CIMS/CFM Data Request Form to the appropriate Datix CIMS/CFM Custodian. Refer to the WA health system Information Register for the list of Datix CIMS/CFM Custodians.

Requestors external to the WA Public health system should send the completed Datix CIMS/CFM Data Request Form to the Datix CIMS/CFM Systemwide Custodian via email to PSSU@health.wa.gov.au.

A copy of the Datix CIMS Data Dictionary, Datix CIMS Incident Classification System, and Datix CFM Issue Categories can be provided to requestors external to the WA public health system upon request.

Appendix 3 – Datix CIMS/CFM Data Release Contract

This contract is designed to protect the confidentiality and integrity of health information and patient data after its release from the Datix CIMS/CFM to an internal (WA health system) or external individual, department or organisation

OBLIGATIONS OF THE REQUESTOR

By signing this contract, the requestor:

- Agrees to maintain the Datix CIMS/CFM information in a confidential and secure manner in the location to which it was originally released.
- Acknowledges that the released Datix CIMS/CFM information remains the property of the WA health system.
- Agrees to, under no circumstances, pass on or divulge the released Datix CIMS/CFM information to a third party without the prior approval of the Custodian(s).
- Agrees not to use the Datix CIMS/CFM information for any purpose other than that for which it was originally requested.
- Agrees that the source of the Datix CIMS/CFM information will be properly referenced whenever it is used in publications.
- Agrees not to copy or store parts or the whole of the released Datix CIMS/CFM dataset in a directory or location that may be accessible to anyone else.
- Agrees not to leave printouts of the released Datix CIMS/CFM dataset in any form in an area accessible to anyone else.
- Agrees to destroy all copies of the Datix CIMS/CFM information and hard copies upon completion of its use for the purpose intended and inform the Custodian(s) of the outcome.

DISCLAIMER

All information/data provided is accurate and up to date at the time of release. The WA health system cannot be held liable for the accuracy of the reports based on the analysis of the data.

CONTRACT

I _____ *(please print)*

of _____ *(department/organisation)*

Acknowledge that I have read and agree to the above provisions of the contract and indicate the intended use of the information requested as follows:

_____

I agree to retain the data in the following location in a secure manner:

_____

Signed:			
Position/Title:		Date:	
Witnessed by:		Position:	
Signature:		Date:	

Office Use Only

Request No:		Received by:	

Appendix 4 – Datix CIMS/CFM Data Release Form

FOR DATA EXTRACTED FROM THE DATIX CIMS/CFM

To be completed be the person extracting the data

DETAILS OF DATA REQUEST

Request number:	
Date received:	
Request description:	
Data supplier name:	
Position:	
Department:	
Organisation:	
Phone:	
Email:	

SPECIFICATIONS OF DATA PROVIDED

Data inclusions:		
Data exclusions:		
Data location:	☐ Attached	
(specify or attached)	☐ Specified	
Date range:		
Known quality issues:		
Definition of variables:	☐ Attached	
(specify or attached)	☐ Specified	
Extraction date:		Total time required:
Completion date:		
Other Comments:		

Signature: *(HE no. if electronic)*		Date:	

This document can be made available in alternative formats on request for a person with disability.