Datix CIMS/CFM
Information Access and Disclosure Model

Release date: December 2016
## Contents

1. Datix CIMS/CFM  
   1.1. Background to Datix CIMS/CFM  
   1.2. Clinical Incident Management and Complaints Management Policies  
2. Datix CIMS/CFM Roles and Responsibilities  
   2.1. Datix CIMS/CFM Data Steward  
   2.2. Datix CIMS/CFM Data Custodian  
3. Datix CIMS/CFM Data Access and Disclosure  
   3.1. Security Profile Access for WA Health Staff  
   3.2. Datix CIMS/CFM Data Extract Requests  
   3.3. Business Intelligence Access via the Data Warehouse  
   3.4. Datix CIMS/CFM Data Access and Disclosure to Non WA Health Personnel  
   3.5. Access Agreements  
      3.5.1. Responsibilities of users  
      3.5.2. Provision of data to parties external to WA Health  
      3.5.3. Requests for data  
      3.5.4. Data release  
4. Definitions  

### Attachment A: Statewide Datix CIMS/CFM Data Access Contract  
### Attachment B: Datix CIMS/CFM Data Request Form  
### Attachment C: Datix CIMS/CFM Data Release Contract  
### Attachment D: DATIX CIMS/CFM Data Release Pro-forma
1. Datix CIMS/CFM

1.1. Background to Datix CIMS/CFM
Clinical Incident Management (CIM) is about improving patient safety by learning from clinical incidents that harm patients and greatly impact on health care delivery. Since 2014, WA Health has been using the web based Datix CIM/Consumer Feedback Module (CFM) as an enterprise system to provide an efficient process for the investigation and management of clinical incidents and complaints.

1.2. Clinical Incident Management and Complaints Management Policies
The governance of the Datix CIMS is captured under the CIM Policy (2015). The purpose of the CIM Policy is to ensure appropriate management of clinical incidents to prevent or reduce future harm to patients/consumers by:

- identifying and treating hazards before they cause harm
- identifying when patients/consumers are harmed and intervening promptly to minimise the harm
- taking preventative actions and sharing lessons learned.

The governance of the Datix CFM is captured under the Complaints Management Policy (2015). The complaints management process is an important strategy for engaging with health consumers and carers and is fundamental to the delivery of quality health care. An effective and efficient complaints management process enables providers to resolve disputes, obtain feedback from consumers and carers and provide strategies for health service improvement.

Contact information
For further information on this document please contact the:
Assistant Director Patient Safety Surveillance Unit (PSSU) and Datix CIMS/CFM Data Custodian WA Department of Health
T: (08) 9222 0284 Email: PSSU@health.wa.gov.au
2. Datix CIMS/CFM Roles and Responsibilities

Overarching responsibility for access, permissions, strategic direction and use of the Datix CIMS/CFM enterprise system is governed by the Data Steward and Data Custodian. While the Data Steward and Data Custodian are responsible for approving access to the Datix CIMS/CFM dataset please note they are not responsible for how the data is analysed, used or when it is disseminated further from trusted data users including data in data warehouses.

2.1. Datix CIMS/CFM Data Steward

The Data Steward of the Datix CIMS/CFM is the Assistant Director General, Purchasing and System Performance, WA Department of Health. The Data Steward’s responsibilities include, but are not limited to:

- setting the strategic direction for the data collection
- ensuring that information and communication technology (ICT) and information management investment for the data collection is aligned to the strategic goals of WA Health
- ensuring projects and initiatives are aligned and coordinated to deliver best value
- ensuring the use, disclosure and access to data meets legislative responsibilities and other arrangements entered into by the State
- endorsing a role based Information Access Control Model that specifies the types of users that can access the data collection and the level of access permitted
- endorsing an Information Disclosure Model which specifies the level of approval required prior to releasing information from the data collection based on the granularity and sensitivity of the information requested
- nominating a Data Custodian for the day-to-day management, operation and support of each data collection.

2.2. Datix CIMS/CFM Data Custodian

The Data Custodian of the Datix CIMS/CFM is the Assistant Director, PSSU, WA Department of Health. The Data Custodian is responsible for the following:

a) Delegated tasks from the Data Steward:

- setting the strategic direction for the data collection
- ensuring that information and communication technology (ICT) and information management investment for the data collection is aligned to the strategic goals of WA Health
- ensuring projects and initiatives are aligned and coordinated to deliver best value
- endorsing a role based Information Access Control Model that specifies the types of users that can access the data collection and the level of access permitted.
b) Data Collection Planning
This includes:
- identifying the information requirements including determining and consulting with key stakeholders and users of the information system
- identifying the data items needed to meet requirements
- identifying existing or overlapping sources of information
- identifying relevant standards, policies and guidelines
- identifying requirements to meet legislative responsibilities and other arrangements entered into by the State
- adhering to organisational metadata, data quality and data security standards
- developing and maintaining system metadata.

c) Data Collection Management and Production
This includes:
- establishing data collection procedures
- ensuring data security and that data meets data quality standards
- ensuring data is not misused or misrepresented
- establishing procedures to permit and review access to information as required by relevant legislation and in accordance with the requirements of the Data Steward
- ensuring data continues to meet business requirements
- developing Information Access and Disclosure Models for endorsement by the Data Steward and ensuring access to and disclosure of data is in accordance with the Information Access and Disclosure Models endorsed by the Data Steward
- extracting data for authorised users
- providing data to authorised recipients
- ensuring the retention, storage and disposal of data is in accordance with relevant legislation and organisational policies.
3. Datix CIMS/CFM Data Access and Disclosure

There are different Datix CIMS/CFM access options available so please read the following sections to fully understand which options are available to you.

- The user profiles for access to Datix CIMS/CFM by WA Health Staff are detailed in section 3.1. A more detailed Security Profile list is held by Health Support Services (HSS) CIMS Support.
- Access permission to the Datix CIMS/CFM system for WA Health Staff is via the Datix HSS CIMS Support System Administrator. Local User Administrator access is provided to Safety, Quality and Performance or Clinical Governance Unit staff to process approved local Datix user access requests.
- For Datix CIMS/CFM extracts access please go to section 3.2.
- For Datix CIMS/CFM Business Intelligence (BI) Access via the Data Warehouse/s please go to section 3.3.
- For non WA health staff requesting Datix CIMS/CFM Data please go to section 3.4.

3.1. Security Profile Access for WA Health Staff

CIMS Notifier
This profile is automatically provided to all WA Health employees, who will be added to the system when the HSS CIMS Support Team runs a synchronisation with the Active Directory. This level of access permits notification of clinical incidents into Datix CIMS, from any location but does not allow access to Datix CFM.

CFM Notifier
This profile may be provided to any WA Health employee who requires access to submit a consumer feedback form in Datix CFM. These users can also notify clinical incidents into Datix CIMS.

Senior Staff
This profile is usually provided to managers who are responsible for the investigation of clinical incidents and consumer feedback events within their area of responsibility. Senior staff access is via ‘Datix CIMS/CFM Request to Amend Access Form’ which is located on the CIMS intranet page and then is sent to the delegated authority for approval, who then forwards it on the local User Admin.

In Datix CIMS this level of access permits:
- Read/write access to all clinical incident module screens, except for the Head of Department screen which is read only.
- Third party comment for incidents outside their area, when invited.
- Read only access to consumer feedback events within their area of responsibility, unless they are requested to participate in the event investigation and therefore have read/write access.
• The user is able to view existing reports and create their own reports. Note: Users with this level of access are unable to view incidents that they have reported outside of their area.

**Consumer Feedback Coordinator**
This profile is usually provided to WA Health employees who coordinate the management of complaints, contacts and compliments (e.g. Customer Service Unit staff, patient/client liaison officers etc).

In Datix CFM this level of access permits:
• Read write access to input data, apply recommendations/ actions, access to assign to or be assigned, analyse data and create reports, access to Dashboard and To Do List and can nominate investigators for that particular Health Service/ Service/ or Service Division.
• Access at a particular Health Service/Service/Service Division or for a feedback record at any other location which they are nominated as Feedback Coordinator.

**CFM Investigator**
This profile is usually provided to WA Health senior staff /managers who may be responsible for the investigation of a consumer feedback event.

In Datix CFM this level of access permits:
• Full read write access to complaints they are invited to comment on and read only for others in the same location only when they are lodged and not inactive, analyse data and create reports, access to Dashboard and To Do List for that particular Health Service/ Service/ or Service Division.
• The user to view existing reports and create their own reports.

**Head of Department**
This profile is usually provided to Directors and Heads of Department who are responsible for endorsing the recommendations, resulting from a clinical incident investigation or consumer feedback event. In Datix CIMS this level of access permits:
• Read/write access to all clinical incident module screens
• The user to view existing reports and create their own reports
• Third party comment for incidents outside their area, when invited.

In Datix CFM this level of access permits:
• Read only access to consumer feedback events within their area of responsibility, unless they are requested to participate in the event investigation and therefore have read/write access.

The user is able to view existing reports and create their own reports. Note: Users with this level of access are unable to view incidents that they have notified outside of their area.
Third Party
This profile may be provided to any health care employee (e.g. allied health staff, medical staff, health information managers, support services managers).

In Datix CIMS this level of access permits:
- The user to access specific clinical incidents when invited
- Read/write access to all clinical incident module screens, except the clinical incident details and investigation screens which are read only.

In Datix CFM this level of access permits:
- The user to access specific consumer feedback events when invited
- Read/write access to all consumer feedback module screens.

The user is able to view existing reports and create their own reports, for the incidents and consumer feedback events that they have been invited to review.

Safety, Quality & Performance (SQP)
This profile is provided to SQP or Clinical Governance Unit (CGU) staff and gives them access to all clinical incidents and consumer feedback events within their area of responsibility. In both Datix CIMS and Datix CFM this level of access permits:
- Read/write access to all clinical incident module screens
- Read/write access to consumer feedback module screens
- The user to view existing reports and create their own report
- Third party comment for incidents outside of their area, when invited.

Statewide Datix CIMS/CFM Access
Statewide Datix access is offered to selected WA Health staff with four access level options available. All access provisions are strictly monitored and require the requestor to sign a Statewide Datix CIMS/CFM Data Access Contract which outlines their obligations with regard to using and disclosing Datix data, please see Attachment A.

Staff who breach confidentiality and security may be subject to disciplinary action and other remedies available through legislative provision such as the Public Service Regulations and the Criminal Code Act 1913. Unauthorised access, use and disclosure of confidential information is misconduct pursuant to the WA Health Code of Conduct and suspected cases may be reported to the Corruption and Crime Commission. Health Service Providers are encouraged to develop internal business processes to manage and monitor their data governance processes and compliance with this policy.
PSSU State-wide Reporting Access to Datix CIMS/CFM (Patient Details De-identified)
This profile is provided to PSSU staff and gives them state-wide access to clinical incidents with de-identified patient details and full access to consumer feedback details.
This level of access permits:
- Read/write access to all clinical incident module screens
- Read/write access to all consumer feedback module screens
- The user to view existing reports and create their own reports.
- The preparation of reports being released to third parties requires the submission and approval of a data request to the Datix CIMS/CFM Data Custodian. Additionally, any report released to a third party requires review and approval from the Data Custodian.

PSSU SAC 1 and Complaints Management with Access to CIMS Patient Details/CFM
This profile is provided to PSSU staff and gives them state-wide access to all clinical incidents, complaints and contact details. This access also allows data entry into Datix CIMS by PSSU of SAC 1 clinical incidents notified by private licensed health care facilities or contracted non-government organisations. This level of access permits:
- Read/write access to all clinical incident module screens
- The user to view existing reports and create their own reports.
- The preparation of reports being released to third parties requires the submission and approval of a data request to the Datix CIMS/CFM Data Custodian. Additionally, any report released to a third party requires review and approval from the Data Custodian.

Other State-wide CIMS Access (WA Health Staff; Patient Details Identified)
This profile is provided to WA Health staff holding state-wide portfolios to enable them to access state-wide clinical incidents details.
This level of access permits:
- Read/write access to all clinical incident module screens
- The user to view existing reports and create their own reports.
- The preparation of reports or data sets being released to third parties requires the submission and approval of a data request to the Datix CIMS/CFM Data Custodian. Additionally, any report released to a third party requires review and approval from the Data Custodian.

State-wide Office of the Chief Psychiatrist Access to CIMS and Contacts Module
This profile is provided to approved external state government staff working closely with WA Health and is undertaken via a memorandum of understanding (MOU) which gives them state-wide access to all clinical incidents and contact details (see section 3.5.2). The Office of the Chief Psychiatrist was granted approval by the Director General to access Datix CIMS and contacts data to enable mandatory reporting to the Chief Psychiatrist. This level of access permits:
- Read/write access to all clinical incident module screens
- The user to view existing reports and create their own reports.
The preparation of reports being released to third parties requires the submission and approval of a data request to the Datix CIMS/CFM Data Custodian. Additionally, any report released to a third party requires review and approval from the Data Custodian.

**Local User Administrator**
This profile is usually provided to a SQP or CGU staff member who has Datix CIMS access for their site/health service/region. This profile only allows access to Datix CIMS/CFM user accounts, in order to process approved user request forms within their area of responsibility. Note: Users who are provided with this profile will be given an additional login and password, to their usual level of access.

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

### 3.2. Datix CIMS/CFM Data Extract Requests
The PSSU provides monthly Datix CIMS/CFM extracts to approved WA Health Services’ Safety and Quality Central Offices. Health Services’ Safety and Quality staff receiving monthly data extracts are responsible for the preparation of these extracts for dissemination, if requested by sites within their Health Service.

The PSSU also provides ad hoc Datix CIMS/CFM extracts to approved agencies, researchers and other parties external to WA Health (e.g. universities, external contractors, non-government organisations and other jurisdictional or national bodies). The level of granularity and intended use of the data requested will determine the approvals required from one or more of the following:

- An appropriate Human Research Ethics Committee (HREC),
- Data Steward,
- Data Custodian,
- Hospital Executive.

### 3.3. Business Intelligence Access via the Data Warehouse
The use of BI data tools to assist in the collation and dissemination of WA Health data has resulted in the establishment of BI Data Warehouses, which currently uses, but is not limited to, the following enterprise systems such as TOPAS, EDIS, TMS and Datix CIMS/CFM.

Requests for access to state-wide Datix CIMS/CFM data feeds from the WA Health Data Warehouse require approval from **ALL** of the following people:

- CIMS/CFM Data Steward
- Datix CIMS/CFM Custodian
- Data Warehouse Custodian.
Once BI access is approved and established, the use of Datix CIMS/CFM data from the state-wide BI Data Warehouse for reports or to populate dashboards requires additional approval from both the Datix CIMS/CFM Data Custodian and the BI Data Warehouse Custodian. This is to ensure that non personal protected internal data or personal (identifiable) data are approved for release with regard to the sensitivity and confidentiality of the data.

Warehouse dashboards are prohibited from:

- Using free text fields without Data Custodian permission.
- Displaying any personal information. The only personal information permitted to be displayed on a dashboard is the CIMS/CFM reference number.
3.4. Datix CIMS/CFM Data Access and Disclosure to Non WA Health Personnel

Access and disclosure of Datix CIMS/CFM data to non WA Health personnel requires different approval processes (see Table 1).

If you have any queries then please contact the Datix CIMS/CFM Data Custodian at PSSU@health.wa.gov.au or on 9222 0284.

### Table 1: Datix CIMS/CFM Data Access and Disclosure to Non WA Health Personnel

<table>
<thead>
<tr>
<th>Purpose for which information is disclosed (external to WA Health)</th>
<th>Non-Personal Published Public</th>
<th>Non-Personal Protected Internal</th>
<th>Personal (Reasonably Identifiable)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorised National Reporting Bodies</td>
<td>No restriction</td>
<td>Approval from Datix CIMS/CFM Data Custodian.</td>
<td>Approval from Datix CIMS/CFM Data Custodian.</td>
</tr>
<tr>
<td>Directly Related Purpose (see section 6.3 of the Information Use and Disclosure Policy 2016)</td>
<td>No restriction</td>
<td>Approval from Datix CIMS/CFM Data Custodian.</td>
<td>Approval from Datix CIMS/CFM Data Custodian AND Datix CIMS/CFM Data Steward.</td>
</tr>
<tr>
<td>Freedom of Information</td>
<td>No restriction</td>
<td>Permitted following consideration and approval of a Freedom of Information application.</td>
<td>Permitted following consideration and approval of a Freedom of Information application.</td>
</tr>
<tr>
<td>Research</td>
<td>No restriction</td>
<td>Approval from Datix CIMS/CFM Data Custodian AND Datix CIMS/CFM Data Steward and ethical approval from a WA Health HREC and site authorisation.</td>
<td>Approval from Datix CIMS/CFM Data Custodian AND Datix CIMS/CFM Data Steward and ethical approval from a WA Health HREC and site authorisation.</td>
</tr>
<tr>
<td>Other legislative requirements (e.g. disclosure under the Child Protection Act)</td>
<td>No restriction</td>
<td>In accordance with relevant legislative, policy and site requirements.</td>
<td>In accordance with relevant legislative, policy and site requirements.</td>
</tr>
<tr>
<td>Other (e.g. disclosure to answer a parliamentary question or in response to an external query for aggregated data).</td>
<td>No restriction</td>
<td>Approval from Datix CIMS/CFM Data Custodian and a WA Health HREC (if required).</td>
<td>Approval from Datix CIMS/CFM Data Custodian AND Datix CIMS/CFM Data Steward and a WA Health HREC (if required).</td>
</tr>
</tbody>
</table>

1 Please see the [WA Health Research Governance Framework website](#) for more details.
3.5. Access Agreements

All data access agreements will be reviewed by the Data Custodian at periods specified with the agreements. Access agreements which may no longer be appropriate will also be reviewed by the Data Steward as required.

The Access Contract for Datix CIMS/CFM (Attachment A) must be completed and approved to gain access to the Datix CIMS/CFM data. This contract involves an acknowledgement that the user will adhere to the Information Disclosure Model and not share information obtained from the Datix CIMS/CFM with third parties without appropriate approvals.

3.5.1. Responsibilities of users

All persons utilising Datix CIMS/CFM data share the following responsibilities:

- using the data in an appropriate manner
- citing the source and currency of the information used
- advising the Data Custodian of any errors or omissions in data received; and
- maintaining confidentiality and security of the information in accordance with conditions of use and relevant legislation.

Information received or accessed through the Datix CIMS/CFM must only be used for the purpose for which it was approved. It should not, under any circumstances, be used in publications or presentations without prior approval in accordance with the Information Disclosure Model.

Users who breach confidentiality and security may be subject to disciplinary action and other remedies available through legislative provisions such as the WA Health Data Breach Response Policy (OD 0564/14), Public Service Regulations and the Criminal Code. A breach of confidentiality and security includes unauthorised access, use and disclosure of confidential information.

3.5.2. Provision of data to parties external to WA Health

For regular provision of/or access to Datix CIMS/CFM data by parties external to WA Health, a contract or MoU between WA Health and the external third party may need to be developed to ensure access to confidential health information by the external party is limited to the use specified and that appropriate safeguards are in place to protect information on the termination of the contract. The MoU should also stipulate that WA Health has the right to audit the third party service provider’s compliance with the contract or MoU.

A thorough risk assessment should be conducted prior to authorising third party access. This may include onsite visits to the facility to ensure WA Health security standards are met in the areas of physical and network security and access and administrative controls. The Data Custodian is responsible for the risk assessment (but may delegate this task).
3.5.3. Requests for data

Requests for access to, or release of data from, the Datix CIMS/CFM should be submitted to the Assistant Director PSSU, (email: PSSU@health.wa.gov.au). Please use the data request form (see Attachment B). Requests will be considered in accordance with the Information Disclosure Model on a case-by-case basis. The required approvals must be sought in line with the Information Disclosure Model.

3.5.4. Data release

Prior to releasing data, the Data Release Contract (Attachment C) must be completed by the requestor. This contract outlines the obligations of the requestor, limitations on usage of the data (including restrictions on further dissemination of the data to third parties) and the manner in which the data will be stored. It allows the Data Custodian to ensure and be confident that the recipient of the data fully understands the conditions of data release and their related obligations. This is particularly important when releasing confidential and/or sensitive data.

A data release pro-forma (Attachment D) should be completed by the person who extracted the information upon supplying the data to the requestor. This form documents the specifications of the data that has been extracted for the recipient, including known issues with data elements and serves as a record for the Data Custodian. The contact person available to handle enquiries from the requestor and/or recipient will be documented on this form. For established routine data requests, a data release pro-forma only needs to be produced on the initial request for data, unless substantial modifications to the data request have been made.

In accordance with the WA Health Guidelines for Release of Data (IC 0208/14), 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 system without the prior appropriate permissions in accordance with the Information Disclosure Model. Confidential or sensitive data must be transferred to the recipient in a secure manner (such as password protecting documents).

Data supplied from the system through the formal request process will have a look and feel common to other WA Health products.

4. Definitions

**Aggregate level data** is summarised and/or categorised data that is analysed and placed in a format that precludes further analysis (for example; in tables or graphs) to prevent the chance of revealing an individual’s identify (individual records cannot be reconstructed).

**Dashboards** refer to the reporting dashboards created using data from the Datix CIMS/CFM system. These dashboards allow users to view information in predefined reports but not to modify data stored within the data repository.
Data collection is a systematic gathering of data for a particular purpose from various sources, including manual entry into an information system, questionnaires, interviews, observation, existing records and electronic devices. This includes both operational data collection and data repositories.

Data repository includes data that is collected from various sources, including operational data collections, for the primary purpose of monitoring, evaluation, reporting and research.

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.

HREC refers to Human Research Ethics Committees. These committees are responsible for the review and approval of research proposals where research involves humans.

Information access refers to the direct access by authorised users (both internal and external to WA Health) to information within WA Health’s data collections. Typically, direct access is gained via a network and/or system login and password to a front-end information system or to a back-end database.

Information disclosure in the context of this model refers to the release of information from WA Health’s data collections to authorised users (both internal and external to WA Health). Information is generally released in the form of hard copy documents, data extracts or electronic medium.

Operational data collection includes data that is collected as part of the day-to-day activities of an area for the primary purpose of tracking and managing the operational aspects of the area. The operational data collection is typically a transaction-based system which contains detailed data elements to represent the activities of the area.

Personal health information pertains to all health information where the identity of a person is apparent or can reasonably be ascertained from the information itself. Information is also personal information if it is reasonably possible for the person receiving the information to identify the individual by using other information that they already hold.

Record level data is usually data at the level of an individual person or clinician. Record level data need not directly identify the patient, but is more vulnerable to re-identification than aggregate data.
Attachment A: Statewide Datix CIMS/CFM Data Access Contract

This contract is designed to protect the confidentiality and integrity of health information accessed from the Datix CIMS/CFM System.

WA Health Staff granted Statewide Datix CIMS/CFM access are required to adhere to strict obligations.

By signing the contract, the user acknowledges and agrees to the following:

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

DISCLAIMER

All information/data provided is accurate and up to date at the time of release. WA Health 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 statewide Datix CIMS/CFM data.

Signed:

Position/Title: Date:

Witnessed by:

Position: Date:

Signature:

Date:

Office Use Only

Request No.: Received by:

Please sign and send a scanned copy of this Statewide Datix CIMS/CFM Data Access Contract along with your Datix CIMS/CFM Statewide Access Form which is located at HSS intranet site: http://intranet.health.wa.gov.au/hin/applications/cims.cfm to the Data Custodian at: PSSU@health.wa.gov.au
# Attachment B: Datix CIMS/CFM Data Request Form

## SECTION 1: REQUEST DETAILS

<table>
<thead>
<tr>
<th>Requestor name</th>
<th>Phone:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Position</td>
<td>Email:</td>
</tr>
<tr>
<td>Work location</td>
<td></td>
</tr>
<tr>
<td>Ethics No.</td>
<td>Request</td>
</tr>
<tr>
<td>Required by (date)</td>
<td>frequency:</td>
</tr>
<tr>
<td>Project Title</td>
<td></td>
</tr>
<tr>
<td>Data Request</td>
<td></td>
</tr>
<tr>
<td>Purpose:</td>
<td></td>
</tr>
</tbody>
</table>

- **Data items/variables required**: *(please be specific and indicate CIMS or CFM)*
- **Description**: *(general summary)*

**Data date range**

<table>
<thead>
<tr>
<th>Specialty</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Sites</td>
<td></td>
</tr>
</tbody>
</table>

State how data will the information be disseminated

**Other**

List persons who will have access to data

**Data retention period** *(data must be deleted after this date)*

<table>
<thead>
<tr>
<th>Duration:</th>
<th>End date:</th>
</tr>
</thead>
</table>

**Requestor**

<table>
<thead>
<tr>
<th>Signature: <em>(HE no. if electronic)</em></th>
<th>Date</th>
</tr>
</thead>
</table>

**Head of Dept**

<table>
<thead>
<tr>
<th>Name</th>
<th>Signature: <em>(HE no. if electronic)</em></th>
<th>Date</th>
</tr>
</thead>
</table>

**Department/Site**

<table>
<thead>
<tr>
<th>Date</th>
<th></th>
<th></th>
</tr>
</thead>
</table>

16
## SECTION 2: APPROVAL DETAILS

<table>
<thead>
<tr>
<th>Request Number</th>
<th>Date received:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comments</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Datix CIMS/CFM Data Custodian Recommendation</th>
<th>Approved</th>
<th>Not Approved</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature (HE no. if electronic)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BI Data Warehouse Custodian Recommendation</th>
<th>Approved</th>
<th>Not Approved</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature (HE no. if electronic)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Data Steward</th>
<th>Approved</th>
<th>Not Approved</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approval Status (as applicable - to be completed by Data Steward)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Signature</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## SECTION 3: COMPLETION DETAILS

<table>
<thead>
<tr>
<th>Date Completed</th>
<th>Date Provided</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revisions Required</td>
<td></td>
</tr>
<tr>
<td>Feedback/Comments</td>
<td></td>
</tr>
</tbody>
</table>
Attachment C: Datix CIMS/CFM Data Release Contract

This contract is designed to protect the confidentiality and integrity of health information and patient data after information is released from the Datix CIMS/CFM System.

OBLIGATIONS OF THE USER

By signing the contract, the user acknowledges and agrees to the following:

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

DISCLAIMER

All information/data provided is accurate and up to date at the time of release. WA Health 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: 

18
**Attachment D: DATIX CIMS/CFM Data Release Pro-forma**

**FOR DATA EXTRACTED FROM DATIX CIMS/CFM**

To be completed by 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
- [ ] Specified

( specify or attached)

#### Date range:
- [ ] Attached
- [ ] Specified

#### Known quality issues

#### Definition of variables:
- [ ] Attached
- [ ] Specified

( specify or attached)

#### Extraction date:  

#### Completion date:  

**Total time required:**

**Other Comments**

**Signature:**

(HE no. if electronic)

**Date:**

---

19