HEALTH INFORMATION EXCHANGE, EDWARD & BUSINESS INTELLIGENCE SECURITY

POLICY©

DOCUMENT SUMMARY/KEY POINTS

- The Health Information Exchange (HIE), Enterprise Data Warehouse for Analysis, Reporting and Decision Support (EDWARD) are data warehouses used across the State and the Reporting database (MSAURPT01) is the Local.
- The **BI Tools** (ie. BusinessObjects - BO, CorVu and Qlik suite) is implemented for the use of the Sydney Children's Hospitals Network and can be accessed by approved staff via the Children's Hospitals' Information Management Portal (CHIMP) on the Application Launcher (AL). Data from the BI Tools come from both HIE and the local Reporting database servers.
- Due to the sensitive nature of data required for reporting purposes it is necessary to identify and review the accessibility, security and privacy of the information stored within the HIE and the Reporting database.
- Staff may have access to these BI Tools by completing the SCHN CHIMP Application Access Form (incorporates general CHIMP Portal access, BI tool access and our Corporate Scorecard).
- Access rights are available to those persons who have a **legitimate business need** to access the data.
- All access accounts will be maintained by MSAU – SDAD and will be reviewed on a periodic basis to ensure the user still requires access to the system.

The use of, disclosure of and/or release of potentially identifiable information must follow the NSW Health Privacy Manual.

Staff accessing HIE, EDWARD & the BI Tools MUST comply with the Information Privacy Code of Practice.

CHANGE SUMMARY

- Due for mandatory review.
- This document replaces SCHN policy 2012-9039 v1
- Updated to accommodate the new tools and systems: recommend reading the entire document.

READ ACKNOWLEDGEMENT

- All SCHN staff wishing to see patient related, finance and human resource information should read and acknowledge they understand the contents of this policy.

TABLE OF CONTENTS

Background 3
Current HIE Process for Reporting 3
Security Components 4
Corporate Information Security 4
Physical Location 4
Responsibilities 4
HIE/EDWARD Coordinator 4
Data Custodian – Divisional Feeder System Managers 5
General Users 5
Information Technology Services 5
Monitoring the Policy 5
Accessibility 6
Operating Availability 6
Access and Authentication 6
Access Rights to the Reporting data 6
HIE / MSAURPT01 System Access 6
Account Access Procedure 6
Review of User Accounts 7
MSAU –SDAD Information Managers 8
Divisional Feeder System Managers 8
General Users 8
Privacy and Confidentiality 8
The Privacy and Personal Information Act 1998 8
NSW Health Privacy Management Plan 8
Information Privacy Code of Practice 8

Access to Sensitive Data *8*
Appendix A: Glossary **11**

Background

The Health Information Exchange (HIE) and soon to be available Enterprise Data Warehouse for Analysis, Reporting and Decision Support (EDWARD) are data warehouses together with our BI Tools; Business Objects (BO), CorVu and Qlik are implemented within Sydney Children's Hospitals Network (SCHN).

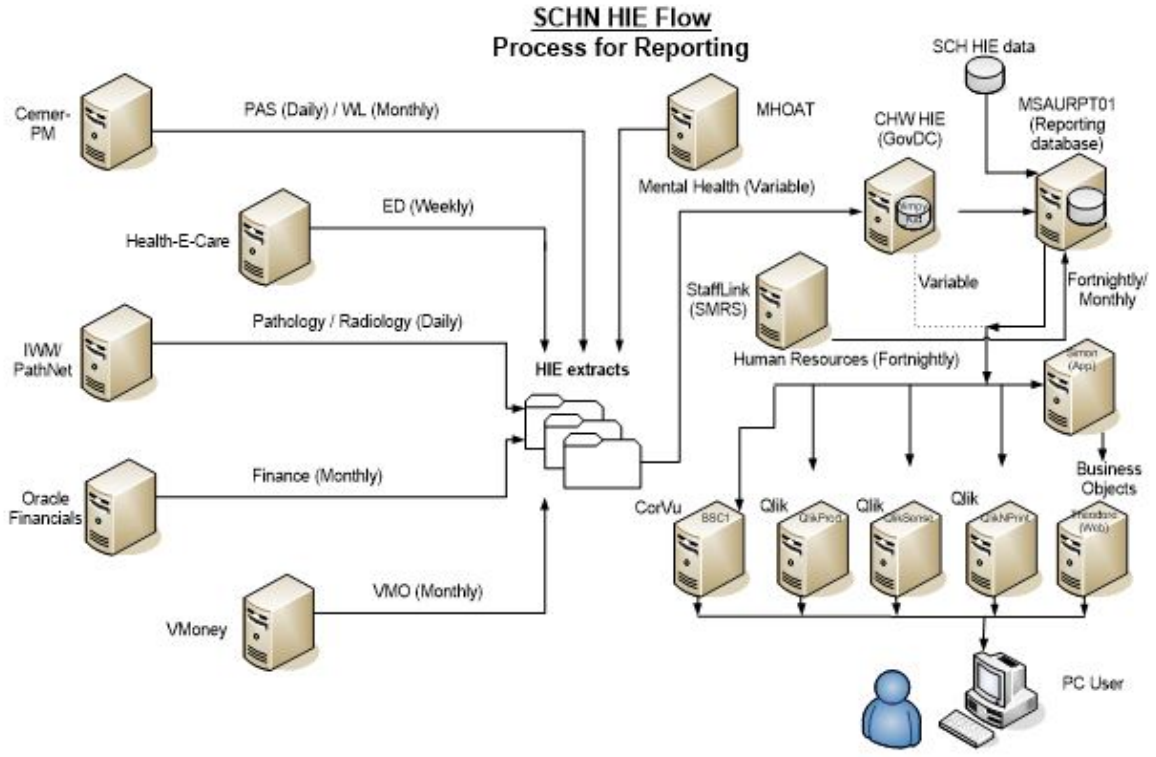
The BI Tools can be accessed by approved staff via the Children's Hospitals Information Management Portal (CHIMP) on our Application Launcher (AL). The CHIMP portal is a central gateway where staff can view various information on a number of categories.

The current HIE data used in our reporting BI Tools aims to standardise information from various source systems within health for analysis and reporting in an easy to use format.

Due to the sensitive nature of data in either the HIE or our local Reporting server (MSAURPT01), it is necessary to identify and review the accessibility, security and privacy of the information stored within, that can be accessed through all the available BI Tools.

The Reporting database (MSAURPT01) stores additional information (not only data elements from HIE) that can also be accessed to meet certain reporting needs, such as Costing information.

Current HIE Process for Reporting



Security Components

The security components mentioned in this policy are:

- Access and authentication
- Availability
- Privacy and Confidentiality
- Data Retention

Corporate Information Security

The development and management of security for the Health Information Exchange, Enterprise Data Warehouse for Analysis, Reporting and Decision Support, the BI Tools and the Reporting server (MSAURPT01) will be undertaken within the context of The Privacy and Personal Information Act 1998, the NSW Health Privacy Management Plan (PD2015_036)) and the Information Privacy Code of Practice 1998.

Physical Location

The HIE and EDWARD is located external to SCHN (GovDC/eHealth) while the BI Tools and MSAURPT01 server is located within the IT Services Department and managed by the Management Support & Analysis Unit (MSAU) – Systems, Data And Development (SDAD) team.

See the IT Services documentation for details on the physical system security.

Responsibilities

HIE/EDWARD Coordinator

The HIE/EDWARD system allows segregation between the administrator and users through the use of access levels controlled with password access.

The HIE/EDWARD Coordinator will be the primary person responsible for general administration and management of the HIE system (at a basic level), EDWARD (when it goes Live), the BI Tools and MSAURPT01.

IT Administrators will be responsible for the in-depth technical maintenance and support required of the HIE, BI Tools and MSAURPT01. This includes software updates, database maintenance, ensuring the interfaces are running smoothly, database creation and low level general operations of the systems.

High level operation of the HIE is the responsibility of eHealth within GovDC.

The HIE/EDWARD Coordinator will coordinate the notification of new upgrades and general maintenance of the HIE, any of the BI Tools and MSAURPT01. This position is the primary point of contact between eHealth (formerly HSS HIE Support), relevant BI Tool Support, and the Network IT department via logging support calls with the appropriate party.

The new EDWARD data warehouse (when it becomes Live) will be maintained externally by eHealth and the Ministry of Health.

Data Custodian – Divisional Feeder System Managers

It is the responsibility of the data custodian to ensure that systems are in place to ensure data extraction from the source system is performed. This person is also responsible for notifying the HIE/EDWARD Coordinator if there are any problems with the extraction of data from the source system (ie. any delays, etc.) Most feeds have an auto-generated email that is sent to the HIE/EDWARD Coordinator and subordinates after each data load from the source system into the HIE, to notify of its successful submission.

Below is a list of the current interfaces to the CHW HIE, and the data custodians/individuals responsible for ensuring they are run on time.

Task	Responsibility	Frequency
ATS and DI interface	Automatic under supervision of the Cerner administrator	Daily
Waiting List Interface	Automatic under supervision of the Cerner administrator	Monthly
Oracle Finance interface	Extraction performed by the Finance Data Custodian. Then automatically loaded into HIE under supervision of the HIE/EDWARD Coordinator and team.	Monthly (after the month has been closed off by the Finance Division)
ED interface	Extraction performed by the ED data manager. Then automatically loaded into HIE under supervision of the HIE/EDWARD Coordinator and team.	Weekly
HR Interface	Managed by eHealth	Fortnightly
V-Money Interface	Managed by eHealth	Monthly
Mental Health	Extraction performed by the MH data collection supervisor. Then automatically loaded into HIE under supervision of the HIE/EDWARD Coordinator and team.	Variable
NAP (formerly DOHRS)	NAPOOS – DOHRS coordinator	Monthly
Pathology / Radiology	Extraction performed by the Cerner data collection supervisor. Then automatically loaded into HIE under supervision of the HIE/EDWARD Coordinator and team.	Daily

There is a dependency on SESLHD for the SCH HIE data and the SCHN HIE/EDWARD Coordinator at CHW will liaise with the SESLHD HIE/EDWARD Coordinator, when and where matters arise.

General Users

Responsible for keeping their login details confidential, and must abide by the conditions of the user agreement.

Information Technology Services

IT Services is responsible for maintaining the low level technical operations of the HIE operating system, maintaining network connections, performing backup and recovery procedures, receiving HELPDESK calls from users and then assigning them, if appropriate to the HIE/EDWARD Coordinator or other MSAU - SDAD staff.

Monitoring the Policy

Compliance with this policy will be monitored by the MSAU – SDAD team. MSAU will take responsibility for the management of the main data warehouse HIE. The BI Tools is partly managed by MSAU and IT Services. Therefore responsibility for monitoring the policy will lie with:

- SCHN Manager of Performance Unit

- HIE/EDWARD Coordinator within Systems, Data & Development team
- IT Services Manager

Accessibility

The accessibility of the current CHW HIE and MSAURPT01 is determined via system availability, timeliness of data by the HIE and data backups reducing the problems of loss of data. SCH HIE has the dependency on SESLHD for the provision of its data.

Operating Availability

The HIE, BI Tools and MSAURPT01 must aim to be available at least 15 hours a day, seven days a week. The system must be available within normal working hours, i.e. 7:30am to 10:30pm, Monday to Friday. Activities that affect the availability and performance of these systems must be scheduled outside of these hours and users must be informed of the unavailability of any of these systems with at least 24 –48 hours' notice, except for emergencies.

Access and Authentication

Access Rights to the Reporting data

HIE / MSAURPT01 System Access

The principle of access rights is the HIE or MSAURPT01 is to be available to those persons who have a **legitimate business need** to access the data. This is a key theme of the NSW Health Electronic Information Policy.

Implicit in this principle is that users have rights to access only specific data areas of the HIE / MSAURPT01 – those areas related to their business need, rather than obtaining access to the whole of the data. These access rights will be determined based on the level of access users have and only being able to see data that they have been given rights to see.

The right to access by staff of SCHN must be confirmed by the user's manager/supervisor and Service Director *as well* as agreed to by the data custodian. The SCHN CHIMP Application Access Form, located under Resources on the existing Management Support & Analysis Unit department intranet page, must be completed to have access granted.

Account Access Procedure

Users will request access to HIE or any of the BI Tools through a central web portal called Children's Hospitals Information Management Portal, or short for CHIMP, using the same form SCHN CHIMP Application Access Form.

This form must be completed by the user and it is the users' responsibility to ensure data they have requested access to be *signed* by the data custodians. Once access has been granted by all the appropriate custodians the form will then be forwarded to MSAU – SDAD team for the account to be created. A login is created and by default the standard Application Launcher icon for CHIMP will be made available to the user. The BI Tools which they can

use will be within this Portal. The user will be notified of their account being created. Passwords are held where applicable in a Sybase/Microsoft SQL Server database for the HIE/MSAURPT01, respectively and/or in the BI Tools security group.

Failure to have approval by their managers and appropriate data custodians will result in delay of account set up for the user.

- Usernames will be assigned and maintained by MSAU – SDAD team.
- Usernames will ideally be the same as the domain username. This will allow for easy identification of users and their use, where applicable.
- Usernames will need to abide by the IT Services User Account Policy.
- The IT system administrator will initially set passwords.
- Passwords must be capable of being changed on a regular basis, in accordance to the IT Services User Account Policy.
- The password must not be visible on the screen at the time of entry.
- The user will continuously be refused entry if login is entered incorrectly. This is designed to prevent unauthorised entry into the systems set up.
- If a user is locked out of their account, they need to either contact IT Services or MSAU – SDAD to have their password reset/account reactivated.

Review of User Accounts

A process has been instigated with the IT Services; in which staff that have left SCHN will have their accounts disabled and will automatically notify MSAU – SDAD team for account termination. User accounts need to be notified and updated monthly to the HIE/EDWARD Coordinator with the following:

- The person having left the Sydney Children's Hospitals Network
- The person having moved to a different position, not requiring access, or requiring a change of access profile
- The person having abused their access privilege.

All accounts related to HIE / BI Tools and CHIMP will be maintained by the HIE/EDWARD Coordinator and team. It will be reviewed on a periodic basis to ensure the user still requires access to the system. This is dependent on IT Services providing notification. The review will entail managers reconfirming that their staff still require access, and users with no activity over a specific period (where applicable) to reconfirm access rights.

Access to Data and Reports

All data held within the HIE / MSAURPT01 servers and accessible through the BI Tools (such as BusinessObjects/CorVu/Qlik) is stored in **read only** format and is available for viewing and for conducting queries.

For many users, access to the information from the HIE or MSAURPT01 will only be in the form of pre-defined reports. Users will access this information through reports/dashboards through the BI Tools (BusinessObjects, CorVu or Qlik).

Functionally, report security is at two levels:

i. A report is available only to specified user groups or user-IDs. Where report access is restricted, users will be prompted for a password in order to view the report.

ii. Each report has internal security where elements of the report are restricted to authorised users only (e.g. a finance report by cost centre).

MSAU –SDAD Information Managers

- Will require whatever access is necessary to prepare standard and ad-hoc reports to fulfil their duties.

Divisional Feeder System Managers

- Access to all data relating to source system as well as relevant error reports.
- Access to all routine reports and ad-hoc reports on source data as deemed appropriate.

General Users

- Users will have access to reports/dashboards and data as defined on their Access Form, based on their business needs.
- Access rights will be determined on a report by report basis.

Privacy and Confidentiality

The Privacy and Personal Information Act 1998

The Privacy and Personal Information Protection Act commenced on 1 July 2000. The Act provides for the protection of personal information and for the protection of the privacy of individuals generally. The Act establishes privacy principles that must be observed by public sector agencies.

NSW Health Privacy Management Plan

The NSW Health Privacy Management Plan consists of 2 documents:

- Privacy Protection Guidelines, which identify how all NSW Health agencies, will comply with the Information Privacy Protection Principles in the Privacy and Personal Information Protection Act.
- Internal Review Guidelines, which provide procedures for the review of certain conduct of an agency, in circumstances where the individual believes that the agency has breached the terms of the Act.

Information Privacy Code of Practice

The NSW Health Privacy Manual has been referenced in the formulation of this security and access Policy.

Staff accessing HIE, EDWARD or any of the BI Tools MUST comply with the Information Privacy Code of Practice.

Access to Sensitive Data

User access to raw data should have the same level of security as in the source system. User access to reports of aggregated data will be determined by the MSAU – SDAD team for each report.

Staff wishing to perform research, an improvement activity or case studies etc please refer to SCHN policy Access to Health Care Records for Research, Quality Activities and Case Studies.

Potentially identifying information

SCHN promotes a policy consistent with the following recommendations:

"Potentially identifiable" data is data from which identifiers, for example, name, address, date of birth etc, have been removed but from which it *might still be possible to identify* an individual indirectly by using an identity number, or code, or other means, to re-identify the individual.

- The use of, disclosure and/or release of potentially identifiable information should be consistent with the Information Privacy Code of Practice.
- Where there is intended disclosure of potentially identifiable information, requests for approval should be directed to the delegated authority. Delegated authorities are:
  - Human Research Ethics Committee (for research projects) **or**
  - Service Improvement Unit (for improvement activities)

Consideration should be given to how the information is analysed, and in particular how it is to be used, interpreted and reported so that the information does not have unintended repercussions or consequences. Retention and security of potentially identifiable information should be addressed in accordance with the information privacy principles and other guidelines in the Information Privacy Code of Practice.

Reporting should not allow the identification of individual participants and must be published in a form which gives due regard to cultural and other sensitivities[1].

Examples of Identifying Information

Medical Record Number

- The Medical Record Number supplied with certain patient records is encrypted within the HIE. The encrypted form of the MRN is known as the Patient Identifier, and is available to users. The unencrypted form, i.e. the supplied MRN, is stored in the HIE database and is only available to authorised users.
- It is anticipated that users will rarely need to view the MRN, but may have access to linked data generated through its use.

Person name

- Person name is to be passed to the HIE. It is proposed that it be collected through the Inpatient Statistics data to allow matching to death data sourced from the Registry of Births, Deaths and Marriages.
- Person name information in HIE will need to be protected in accordance with the Information Privacy Code of Practice. Access will only be possible with the approval of the relevant SCHN Data Custodian and would generally only be made available in exceptional circumstances.

Patient address

- Patient address is supplied with most patient data. Patient address is identifying information and must be removed from de-identified data user views with the exemption of postcode. Higher-level derived address items may be included in these views; these items may include Postcode and Statistical Local Area (SLA).

References

1. Ethical Management of Health Information Discussion Paper, NSW Department of Health
2. NSW Health Policy Directive Electronic Information Security Policy - NSW Health: http://www0.health.nsw.gov.au/policies/pd/2013/pdf/PD2013_033.pdf (accessed Sept 2015)
3. NSW Health Privacy Manual for Health Information: http://www.health.nsw.gov.au/policies/manuals/Pages/privacy-manual-for-health-information.aspx (accessed Sept 2015)

Appendix A: Glossary

Availability

- The characteristic of data, information and information systems being accessible and useable on a timely basis in the required manner.

Confidentiality

- The characteristic of data and information being disclosed only to authorised persons, entities and processes with a right to know at authorised times and in an authorised manner.

Data

- A representation of facts, concepts, or instructions in a formalised manner suitable for communication, interpretation or processing by electronic or manual mean.

Database administrator

- The person responsible for managing all activities in support of the database. This includes database availability, backups, software loads and security management.

Data Custodian

- A person or organisation who can determine the contents and use of data collected, stored, processed or disseminated by that party regardless of whether or not the data was acquired from another owner or collected directly from the provider.

Data Integrity

- The characteristic of data and being accurate and complete and the preservation of and completeness. In other words, data being accurate, complete and reliable.

Data provider

- A person or organisation providing data either directly or indirectly to the data owner.

GovDC

- Government Data Centre where State owned systems will be hosted from.

Information

- The meaning assigned to the data by means of conventions applied to that data.

Information systems

- Computers, communication facilities, networks, data and information that may be stored, processed, retrieved or transmitted by them, including programs, specifications and procedures for their operation, use and maintenance.

System administrator

- The person responsible for managing user related activities in support of users and the HIE/MSAURPT01. They are in regular contact with the database administrator.

Security processes

- The measures, practices and procedures relating to the security of information systems including both logical and physical security.