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

Data Linkage Branch

Confidentiality and Security Standards in the Data Linkage Branch (abridged)

better health ▪ better care ▪ better value

Contents

Purpose

This document is an abridged list of the standards used by the Data Linkage Branch (DLB) to manage and secure confidential information.

Confidentiality and Security Standards

The standards described in this document enforce parts of the framework described by the WA Data Linkage Branch Access and Charging Policy.

The Department of Health (DOH) via Health Support Services (HSS) implements a number of security and access standards with which DLB comply. This document describes additional security standards enforced by DLB.

Personnel

Employees and Contractors

- All DLB staff must abide by DOH policies including the IT Acceptable Use Standards.
- All DLB employees and contractors must sign the DLB Confidentiality Agreement.
- All DLB employees and contractors are responsible for data security in the DLB.

Visitors

- All non-DOH visitors to the DLB must sign in with the security staff at the Commissionaire's desk and be issued with a visitor's badge.
- Visitors to the DLB must be accompanied by a DLB employee or contractor at all times.
- All visitors must be escorted from the floor at the conclusion of their visit.
- Visitors shall not have access to DLB data or systems, unless authorised by the Program Manager.

Environment

Physical Environment

- DLB facilities must be located in a secure area, with security cards (or similar authentication) required for access.
- Physical access to DLB Servers must be limited to only the DLB Systems Team and HSS Staff.
- The location of the Linkage and Client Services Teams within DLB must be physically separate.

Personal Computers

- DLB must not store any identified or de-identified data on DLB (or other) personal computers.

Mobile Devices (Laptops/Tablets)

- DLB must not store any identified or de-identified data on DLB or personal mobile devices.

- Any visiting analyst using their own mobile device must leave it at DLB between visits. Any such mobile device must be formatted at the completion of analysis.
- Mobile devices not approved by HSS may not be directly connected to the DOH network.

Software Updates

- Where software updates are available from the vendor, a schedule for applying these must be maintained.

Printed and Portable Media

- Portable media, such as CDs, DVDs, tapes, USB thumb drives and paper copies used to store confidential data must be placed in the DLB safe or locked in the appropriate filing cabinet in the DLB area.
- Data must never be faxed or e-mailed.
- Redundant physical media that may contain confidential data must be destroyed using the appropriate facilities (e.g. confidential paper disposal bins; CD/DVD shredder).

Data Transfer and Handling

Incoming

- Incoming data must be provided in a secure manner.
- Incoming identifying data must be provided only to the Linkage Team and promptly checked for content.
- Incoming service data must be provided only to the Client Services Team and promptly checked for content.
- It is not permitted to receive confidential data by email.

Outgoing

- Data released must meet all requirements specified by the relevant policies and legislation (including the DLB Access and Charging Policy).
- Data released must be subject to quality assurance protocols before release.
- Data Collections' original record IDs must not be released without specific approval of the applicable Data Custodian(s). DLB-generated record and person IDs (Root or LPNO) must be used instead.
- Roots and LPNOs must be encrypted prior to release, unless written authorisation is granted by the Program Manager to the contrary.
- All linked data extracts must be provided via secure online transfer, such as MyFT or SUFEX. If this is not possible, they are hand-delivered or sent via registered courier. Data must be encoded before being dispatched, with any passwords being provided via a separate channel.
- It is not permitted to e-mail confidential data.

Backup

- Regular encrypted backups of all data and systems must be taken, with a current subset held in a suitable, secure, off-site storage location.

Access to Servers and Data

- Passwords are required for end-users to access the DLB servers.
- Passwords must follow the security protocol and users must change their passwords every 6 months.
- A class of user should be granted only the minimum level of access to directories and files on the server required for their role.
- All servers and restricted applications must require the user to log in with a password.
- Passwords must meet or exceed DOH requirements.
- Steps must be taken to detect and/or prevent unauthorised access.
- Access to data will only be granted to users where such access is required for them to perform their work.

Document Control Sheet

Contact details for enquiries and proposed changes:

Name	Tom Eitelhuber
Designation	Manager, Data Linkage Systems Data Linkage Branch
Phone	(08) 9222 2371
Fax	(08) 9222 4236
E-mail	Tom.Eitelhuber@health.wa.gov.au

Definitions

Term	**Definition**
Client Services Team	DLB team comprising Project Manager, Senior Project Officers, Project Officers and related positions
Confidential data	Any data that carries a duty of non-disclosure for any purpose other than that for which it was provided. Includes both identifying and non-identifying data.
Data Collection	Refers to the systematic gathering of data for a specific purpose from various sources, including manual entry into an application system, questionnaires, interviews, observation, existing records and electronic devices. It includes collections of patient, corporate, financial and workforce information. This includes both operational data collections and data repositories.

Data Custodian	The person(s) responsible for the day-to-day management of data from a business perspective. The Data Custodian aims to improve the accuracy, usability and accessibility of data within the data collection.
Data Delivery Team	DLB team comprising Data Coordinators. Data Analysts and related positions
DLB	Data Linkage Branch
DOH	Department of Health (WA)
Encryption	The process of converting information or data into a code, especially to prevent unauthorised access.
HSS	Health Support Services
Identifying data	Data that overtly reveals a person's identity; this is the type of data handled by the Linkage Team and stored on the Linkage server. Also known as "identified data" and "demographic data".
Linkage Team	DLB team comprising Manager Data Linkage Systems, Principal Linkage Officers, Senior Linkage Officers, Linkage Officers and related positions
LPNO	The "record number" assigned by DLB to each record, prior to undertaking the linkage process
Root	The "person number" created via DLB's linkage process to indicate where records are thought to belong to the same person; also known as a "linkage key"
Server	A computer device that provides functionality for other devices.
Service data	Data that does not overtly reveal a person's identity; this is the type of data handled by the Data Delivery Team and is ultimately provided to applicants for DLB services. Also known as "de-identified data" and "content data".
Systems Team	DLB team comprising Senior Programmers, Programmers, Systems Administrators, Software Developers and related positions

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