Independent Hospital Pricing Authority

Confidential Data Management Policy

May 2022

IHPA

Confidential Data Management Policy – Version 4.0 May 2022

Table of contents

Acronyms and abbreviations

CEO	Chief Executive Officer
DLM	Dissemination Limiting Marker
IHPA	Independent Hospital Pricing Authority
The Addendum	Addendum to the National Health Reform Agreement 2020–25
The NHR Act	*National Health Reform Act 2011* (Cwlth)
This Policy	*Confidential Data Management Policy*

Definitions

Confidential jurisdictional information	Any economic projections of jurisdictions; or where there is mutual understanding and agreement between the Independent Hospital Pricing Authority (IHPA) and the jurisdiction that the information has been provided in confidence. If confidential jurisdictional information is delivered orally, such as through discussions, there should be mutual understanding and agreement between IHPA representatives and the jurisdictional representative that the information is being provided in confidence.
IHPA representatives	The Chief Executive Officer of IHPA, Pricing Authority Members, IHPA staff, contractors and consultants.
Pricing Authority	The governing body of IHPA established under the *National Health Reform Act 2011* (Cwlth).

1. Executive summary

1.1 Background

The Addendum to the National Health Reform Agreement 2020–25 (the Addendum) outlines the Independent Hospital Pricing Authority's (IHPA) determinative functions, including to develop projections of the national efficient price for a four year period on an annual basis and provide confidential reports on these projections to the jurisdictions. To undertake its determinative functions, IHPA relies on the provision of confidential jurisdictional information from the Commonwealth and states and territories.

Clauses B66–B81 of the Addendum stipulate that IHPA will develop rolling three year data plans to indicate its future data needs, and that jurisdictions must provide IHPA with the data required to carry out its functions in accordance with its data plans.

IHPA has a comprehensive approach to data and information protection informed by national and international standards and best practice, and advances in technology. This approach ensures compliance with legislation and contractual arrangements and that personnel are screened and trained, processes are transparent, project and analysis methods are robust, data and information management is safe and secure, de-identified data is used within the scope of the legislative requirements, and output is safe. Based on this approach, IHPA has developed a system of continuously updating and improving safeguards to protect information and to meet evolving organisational and technical demands.

Confidential jurisdictional information provided to IHPA is protected by provisions in Australian legislation and frameworks, policies and contracts. Legislative protections include the *National Health Reform Act 2011* (Cwlth) (the NHR Act), the Addendum, the *Public Governance Performance and Accountability Act 2013* (Cwlth), the *Archives Act 1983* (Cwlth), the *Privacy Act 1988* (Cwlth), the *Protective Security Policy Framework* and the *Digital Transition Policy*. IHPA also elects to comply with state and territory data and information protection legislation.

1.2 Purpose

The purpose of the *Confidential Data Management Policy* (this Policy) is to advise jurisdictions of the processes and controls adopted by IHPA in managing confidential jurisdictional information. This Policy outlines the limited and prescribed purpose for which IHPA can collect and analyse confidential jurisdictional information and the controls in place to prevent unauthorised access to confidential jurisdictional information and disclosure to unauthorised parties. This includes the processes and controls for requests, access, handling, use, classification, storage, release and disposal of confidential jurisdictional information.

This Policy applies to all confidential jurisdictional information received from jurisdictions by IHPA representatives, including the Chief Executive Officer (CEO) of IHPA, Pricing Authority Members, IHPA staff, contractors and consultants.

1.3 Review

The Pricing Authority and CEO of IHPA will review this Policy, including associated documentation, annually or as required.

This Policy was last reviewed in May 2022.

2. Management of confidential jurisdictional information

Confidential jurisdictional information provided to IHPA is an important asset. IHPA is committed to providing the best possible safeguards to protect this asset and ensuring that stakeholders are aware of the nature and scope of these safeguards. This Policy contributes to these safeguards by providing a specific focus on managing confidential jurisdictional information.

Serious penalties may apply for inadvertent or deliberate breaches to legislation, contracts and IHPA policies relating to the protection and use of confidential jurisdictional information. For IHPA these include criminal and civil remedies, and loss of the social licence to operate. For individual personnel, including current and former IHPA officials, penalties may include disciplinary action, termination of employment, and criminal and civil remedies.

Detailed below is a summary of the processes and controls in place to ensure the effective management of confidential jurisdictional information held by IHPA.

2.1 Requests

Where a jurisdiction provides confidential information to IHPA, the jurisdiction must identify the information by using the relevant classification schema specified in the request. Further details of classification schema that may be used can be found in IHPA's Three Year Data Plan.

2.2 Access, handling and use

IHPA takes all reasonable steps to ensure that confidential jurisdictional information remains confidential. IHPA only discloses confidential jurisdictional information to external agencies or individuals as permitted under legislation, contract consent or policy. IHPA does not copy or record confidential jurisdictional information other than for the purpose of carrying out its functions under the NHR Act and the Addendum.

IHPA only discloses confidential jurisdictional information to its officers and employees on a need-to-know basis for the purpose of carrying out IHPA's functions. IHPA ensures its officers, employees, consultants and third parties are aware of the legislative and policy requirements for confidential jurisdictional information. The requirements for consultants and third parties are set out in the IHPA *Consultant Access to IHPA Protected Data Rules*.

2.3 Classification

IHPA is required to classify information it receives and, where necessary, ensure that information is handled by staff with the appropriate security clearance in line with the *Protective Security Policy Framework*. This policy sets out the system for the control and handling of security classified information and the details of the documents received and copies retained.

IHPA maintains a classified document register for all 'TOP SECRET' and 'SECRET' materials produced or received.

To ensure compliance, IHPA maintains a register of the security vetting clearances held by staff.

2.3.1 Dissemination Limiting Marker

IHPA identifies confidential jurisdictional information by labelling it with the appropriate Dissemination Limiting Marker (DLM).

DLMs are markings for information where disclosure may be limited or prohibited by legislation, or where it may otherwise require special handling. As outlined in the *Protective Security Policy Framework*, IHPA is responsible for determining the appropriate protections to be applied to information bearing DLMs (other than 'Sensitive: Cabinet'), whilst ensuring that the principles of information security practice are applied. The following four categories of DLMs are used:

- Unofficial
- Official
- Official: Sensitive
- Protected.

IHPA selects DLMs (other than 'Sensitive: Cabinet') on a case-by-case basis. In most cases confidential jurisdictional information is marked 'Official: Sensitive'.

2.4 Storage

IHPA uses authorised systems and processes for managing information and records in all formats, aiming to manage digital records in an electronic format in alignment with the *Digital Transition Policy*.

All information received from jurisdictions is stored securely both electronically (on the Secure Data Management System, IHPA's secure access controlled cloud based data storage network) and physically (locked cabinets).

2.5 Release

IHPA has developed a *Data Access and Release Policy,* which outlines its principles and processes to release information.

2.6 Disposal

When the confidential jurisdictional information is no longer required, it is stored or disposed of in accordance with IHPA's Record Authority or relevant General Record Authorities issued by the National Archives of Australia.

3. Compliance

3.1 Internal controls

IHPA proactively manages the confidential information provided by jurisdictions with risk mitigation. In addition to the controls outlined in Chapter 2 of this Policy, IHPA:

- documents policies, plans and procedures for the management of confidential jurisdictional information and records
- provides security awareness training to staff at their induction and at regular intervals, as well as to contractors and consultants before they can access data and information
- maintains a 'Designated Security Assessed Position Register' which details IHPA staff and representatives granted a security clearance by the Australian Government Security Vetting Agency
- has established an Audit, Risk and Compliance Committee that meets regularly to discuss issues, with a Chairperson independent to IHPA
- arranges regular internal and external security audits of its operations
- regularly reports on compliance to the CEO of IHPA, the Pricing Authority and internal committees.

3.2 Assurance

IHPA assesses the effectiveness of internal controls by undertaking regular compliance monitoring through:

- routine verification of compliance with the IHPA policies, plans and procedures through internal audits
- internal monitoring of compliance with internal controls by the CEO of IHPA
- annual reporting of compliance with mandatory *Protective Security Policy Framework* requirements to the Minister of Health
- conducting regular data assurance audits.

Independent Hospital Pricing Authority

Eora Nation, Level 12, 1 Oxford Street
Sydney NSW 2000

Phone 02 8215 1100
Email enquiries.ihpa@ihpa.gov.au
Twitter @IHPAnews

www.ihpa.gov.au

IHPA