

Independent Hospital Pricing Authority

# Management of Confidential Jurisdictional Information Protocol

April 2021



IHPA

## Management of Confidential Jurisdictional Information Protocol – Version 3.0 April 2021

© Independent Hospital Pricing Authority 2021

This publication is available for your use under a Creative Commons BY Attribution 3.0 Australia licence, with the exception of the Independent Hospital Pricing Authority logo, photographs, images, signatures and where otherwise stated. The full licence terms are available from the Creative Commons website.



Use of Independent Hospital Pricing Authority material under a Creative Commons BY Attribution 3.0 Australia licence requires you to attribute the work (but not in any way that suggests that the Independent Hospital Pricing Authority endorses you or your use of the work).

*Independent Hospital Pricing Authority material used 'as supplied'.*

Provided you have not modified or transformed Independent Hospital Pricing Authority material in any way including, for example, by changing Independent Hospital Pricing Authority text – then the Independent Hospital Pricing Authority prefers the following attribution:

*Source: The Independent Hospital Pricing Authority*

# Table of contents

<b>Acronyms and abbreviations .....</b>	<b>4</b>
<b>Definitions .....</b>	<b>4</b>
<b>1. Executive summary .....</b>	<b>5</b>
1.1 Background.....	5
1.2 Purpose .....	5
1.3 Review .....	5
<b>2. Management of confidential jurisdictional information .....</b>	<b>6</b>
2.1 Request .....	6
2.2 Access, handling and use .....	6
2.3 Classification.....	6
2.4 Storage .....	7
2.5 Release.....	7
2.6 Disposal .....	7
<b>3. Compliance .....</b>	<b>8</b>
3.1 Internal controls.....	8
3.2 Assurance .....	8

# Acronyms and abbreviations

<b>CDR</b>	Classified Document Register
<b>CEO</b>	Chief Executive Officer of the Independent Hospital Pricing Authority
<b>DLM</b>	Dissemination Limiting Marker
<b>FOI Act</b>	<i>Freedom of Information Act 1982 (Cwlth)</i>
<b>IHPA</b>	Independent Hospital Pricing Authority
<b>SDMS</b>	Secure Data Management System
<b>The Addendum</b>	Addendum to the National Health Reform Agreement 2020–25
<b>The Protocol</b>	IHPA Management of Confidential Jurisdictional Information Protocol

# Definitions

**Confidential jurisdictional information**

Any economic projections of jurisdictions; or where there is mutual understanding and agreement between IHPA and the jurisdiction that the information has been provided in confidence.

If confidential 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**

Chief Executive Officer, 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

Clause B72 of the Addendum to the National Health Reform Agreement 2020–25 (the Addendum) states that jurisdictions must provide the Independent Hospital Pricing Authority (IHPA) with the data required to carry out its functions in accordance with its Three Year Data Plan.

Clause B24(h) of the Addendum requires IHPA to develop four year projections of the national efficient price and to provide these projections as confidential reports to the Commonwealth and states and territories. IHPA relies on confidential jurisdictional information to meet this requirement.

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 that personnel are screened and trained, processes are transparent, project and analysis methods are robust, data and information management is safe and secure, compliance with legislation and contractual arrangements, de-identified data is used within the scope of the legislative requirements, and that 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 *Public Governance Performance and Accountability Act 2013* (Cwlth), the *Archives Act 1983* (Cwlth), the *Privacy Act 1988* (Cwlth), the *National Health Reform Act 2011* (Cwlth), the Addendum, the *Australian Government Protective Security Policy Framework* (Cwlth) and the Australian Government Digital Transition Policy. IHPA also elects to comply with state and territory data and information protected legislation.

The Protocol outlines the limited and prescribed purpose for which IHPA can collect and analyse confidential jurisdictional information and the processes and controls in place to prevent unauthorised access to confidential jurisdictional information and disclosure to unauthorised parties.

## 1.2 Purpose

The purpose of the Protocol is to advise jurisdictions of the processes and controls adopted by IHPA in managing confidential jurisdictional information. This includes the processes and controls for requests, access, handling, use, classification, release, storage and disposal of the confidential jurisdictional information.

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

## 1.3 Review

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

The Protocol was last reviewed in April 2021.

## 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. The Protocol 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, contract and IHPA policies and protocols 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 Request

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 the 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 *National Health Reform Act 2011* (Cwlth) 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 IHPA's *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 (except 'Sensitive: Cabinet'), whilst ensuring that the following principles of good information security practice are applied. The following four categories of DLM are used:

- Unofficial
- Official
- Official: Sensitive
- Protected.

IHPA selects DLMs (other than 'Sensitive: Cabinet') on a case-by-case basis. In the 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 *Australian Government Digital Transition Policy*.

All information received from jurisdictions is stored securely both electronically (on the Secure Data Management System (SDMS), 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 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 Protocol, IHPA:

- documents policies, plans and procedures for the management of 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 Executive Officer
- 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**

**Level 6, 1 Oxford Street  
Sydney NSW 2000**

**Phone 02 8215 1100  
Email [enquiries.ihpa@ihpa.gov.au](mailto:enquiries.ihpa@ihpa.gov.au)  
Twitter [@IHPAnews](https://twitter.com/IHPAnews)**

**[www.ihpa.gov.au](http://www.ihpa.gov.au)**



**IHPA**