Independent Hospital Pricing Authority

Management of Confidential Jurisdictional Information Protocol

Version 2.3 June 2019

Management of Confidential Jurisdictional Information Protocol – Version 2.3 June 2019

Table of Contents

Acronyms and abbreviations

CDR	Classified Document Register
CEO	Chief Executive Officer
DLM	Dissemination Limiting Marker
FOI Act	*Freedom of Information Act 1982*
IHPA	Independent Hospital Pricing Authority
NHRA	National Health Reform Agreement
NEP	National Efficient Price
PSPF	Protective Security Policy Framework
SDMS	Secure Data Management System
the Act	*National Health Reform Act 2011*
The Protocol	*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.

1. Executive summary

1.1 Background

Clause B93 of the National Health Reform Agreement (NHRA) states that jurisdictions will provide IHPA with the data required to carry out its functions in accordance with its Three Year Data Plan.

Clause B3(h) of the NHRA requires IHPA to develop four year projections of the National Efficient Price (NEP) and provide these as confidential reports to the Commonwealth and states and territories. IHPA requires confidential jurisdictional information to support this work.

Where information provided by jurisdictions contains confidential jurisdictional information, IHPA has developed this protocol – the IHPA *Management of Confidential Jurisdictional Information Protocol* (the Protocol) – to outline the processes and controls in place which prevent unauthorised access to, and disclosure of, the confidential jurisdictional information to third parties which are not authorised to receive such information under the NHRA, the *National Health Reform Act 2011* (the Act) or pursuant to any other law.

This Protocol is supported by other existing frameworks, policies and protocols within IHPA, in particular IHPA's internal *Protective Security Framework*. A range of policies and procedures sit underneath this framework and together they provide a comprehensive framework for managing and protecting information collected and handled by IHPA.

As an Australian Government agency subject to the *Public Governance Performance and Accountability Act 2013*, IHPA must have appropriate systems of risk oversight and management in place and internal controls which promote the proper use and management of public resources. IHPA is also required to comply with the Australian Government Protective Security Policy Framework (PSPF) and IHPA's internal protective security framework is aligned to the PSPF to the extent that the Act allows.

IHPA is also bound by other legislative requirements including the *Archives Act 1983* (Archives Act), the *Privacy Act 1988* (Privacy Act) and the *Freedom of Information Act 1982* (FOI Act). IHPA will comply with any requests for information release in accordance with its legal obligations and the principles of information release as prescribed in the Archives Act, the Privacy Act and the FOI Act. Certain exemptions exist under the FOI Act and IHPA will apply an exemption where it is appropriate to do so.

1.2 Purpose

The purpose of this Protocol is to advise jurisdictions of the processes and controls adopted by IHPA in managing confidential jurisdictional information as part of IHPA's rolling Three Year Data Plan (used for its four year projections of the NEP).

This includes the controls IHPA applies to the request, access, handling, use, classification, release, storage and disposal of the confidential jurisdictional information.

1.3 Scope

The Protocol applies to all confidential jurisdictional information received from jurisdictions by IHPA representatives, including the Chief Executive Officer (CEO), Pricing Authority Members[1], IHPA staff, contractors and consultants.

1.4 Review

The CEO will review the Protocol annually or as required. This review will ensure the Protocol remains current to sufficiently support IHPA in managing confidential jurisdictional information.

The Protocol was last reviewed in June 2019.

[1] The Pricing Authority refers to the governing body of IHPA

2. Management of confidential jurisdictional information

Anyone accessing protected Pricing Authority information[2] is bound by the secrecy provisions set out at Part 4.14 of the Act. In essence, these provisions provide that such information can only be disclosed for limited and prescribed purposes.

In addition, IHPA staff and representatives are required to manage the information collected and handled by IHPA in accordance with the policies and procedures included under IHPA's internal *Protective Security Policy Framework*. IHPA has developed policies which cover various aspects of information security management, including the *Information Security Policy and Operations Security Policy*. Policies relating to information classification and access, and information release also manage who, how and in what circumstances information collected by IHPA can be accessed. For example, the IHPA *Third Party ICT and Data Management Controls* sets out the conditions which IHPA requires to be satisfied prior to protected Pricing Authority information being provided to a third party.

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

2.1 Request

IHPA's Three Year Data Plan outlines the data required from jurisdictions to enable IHPA to undertake its functions under the Act. Clause B93 of the NHRA requires jurisdictions to provide data requested by IHPA.

Where a jurisdiction provides confidential information pursuant to a request from IHPA, the jurisdiction must identify the information accordingly.

2.2 Access, handling and use

IHPA will take all reasonable steps to ensure that the confidential jurisdictional information remains confidential. IHPA will not disclose the confidential jurisdictional information to any person outside the organisation, other than where IHPA is permitted to do so under the NHRA, the Act or any other law or where IHPA has obtained the consent of the relevant jurisdiction. IHPA will not copy or record the confidential jurisdictional information other than for the purpose of carrying out its functions under the Act, the NHRA or any other law.

IHPA will only disclose the confidential jurisdictional information to those of its officers and employees who have a need to know for the purpose of carrying out IHPA's functions under the Act, the NHRA or any other law. IHPA will ensure officers and employees are aware that the confidential jurisdictional information must be kept confidential.

IHPA's *Third Party Usage of IHPA Protected Data Rules* sets out the rules contractors and consultants must comply with before getting access to data and information collected by IHPA for

[2] See section 5 of the *National Health Reform Act 2011*

its functions under the NHRA and the Act. The document as well as this Protocol will apply to the access, handling and use of confidential jurisdictional information.

In accordance with the *Third Party Usage of IHPA Protected Data Rules*, IHPA facilitates access to IHPA Protected Data via the Secure Data Management System (SDMS). SDMS access can be accessed at IHPA's office in Sydney or offsite using the third party suppliers own hardware. The following data access model outlines this process.

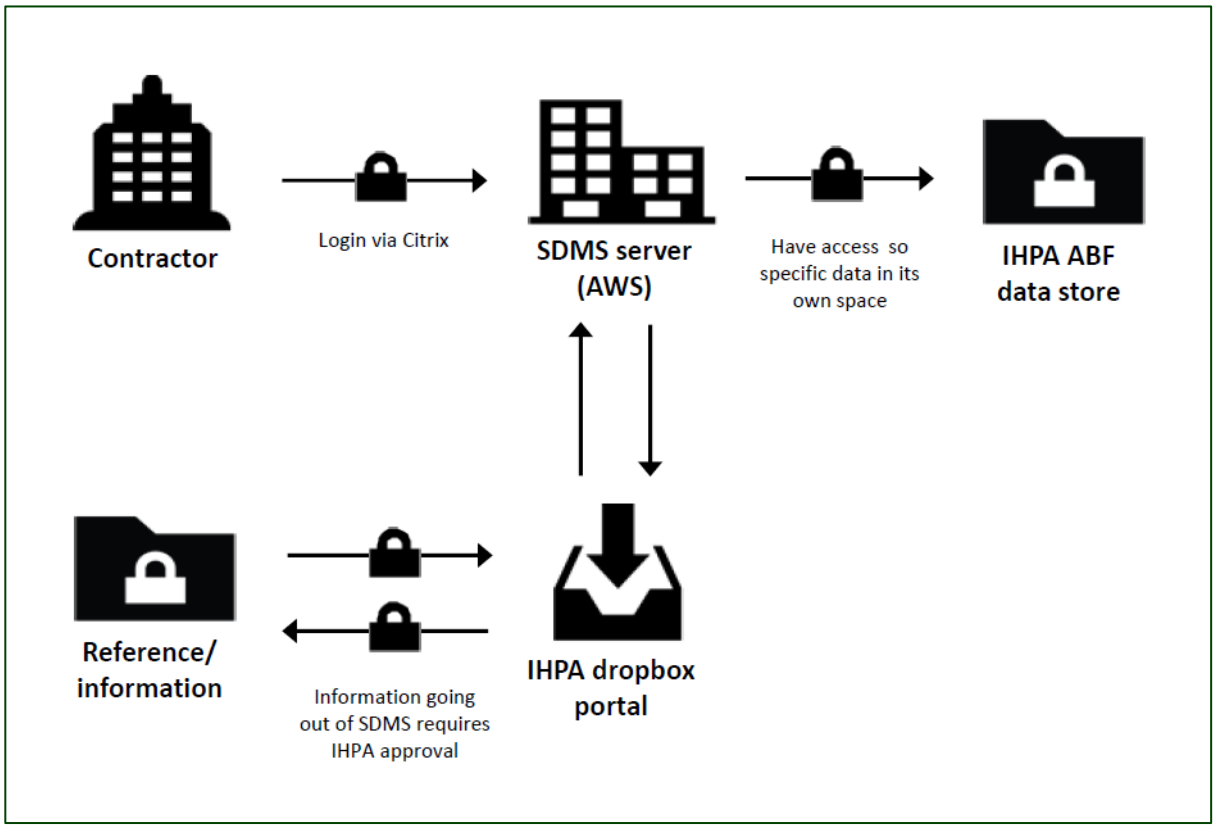

Figure 1. IHPAs Protected Data Access Model

Any alternatives to this model requires, comprehensive justification and a risk assessment and must be pre-approved by the IHPA CEO in writing.

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 PSPF.[3]

To ensure it is complying with this obligation, IHPA maintains a register of security vetting clearance held by staff. Further, IHPA's *Information Security Policy* sets out the system for the control and handling of security classified information in accordance with the PSPF. IHPA maintains a classified document register (CDR) for all 'TOP SECRET' and 'SECRET' materials produced or received. The CDR includes details of the documents received and all retained copies.

[3] The information is set out in '9 Access to information' of the *Australian Government Personnel Security Protocol* (v2018.2), at <http://www. https://www.protectivesecurity.gov.au/information/access-to-information/Documents/pspf-infosec-09-access-information.pdf>

IHPA has identified that confidential jurisdictional information must be subject to additional protections and classifies this information as being sensitive data.

2.3.1 Dissemination Limiting Marker

The definition of 'Confidential' information under the PSPF does not align with legal definitions of 'confidential' information nor is it aligned to the definition used in this document. However, IHPA will identify such information as confidential to all recipients, 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 PSPF, 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 five categories of DLM are used:

- Unofficial
- Official
- Official: Sensitive
- Protected

IHPA will choose whether to use DLMs (other than 'Sensitive: Cabinet') on a case-by-case basis. With regard to confidential information provided by jurisdictions, in the majority of cases it will be marked 'Sensitive'.

The presence or absence of such a marking will not affect a document's status under the *Freedom of Information Act 1982* (FOI Act).

2.4 Storage

IHPA uses authorised systems and processes for managing information and records in all formats, aiming to manage digital records in 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 the principles and processes to be followed by IHPA with regard to the release of information.

Confidential information received from a jurisdiction will not be disclosed to any third parties unless IHPA is permitted to do so pursuant to the NHRA, the Act or any other law, without consulting with the jurisdiction which provided the information (including FOI requests).

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 is proactive in managing confidential information provided by jurisdictions and minimising the risk of breaches. In addition to the controls outlined in section 2, IHPA takes the following steps:

- Documented policies, plans and procedures for the management of information and records.
- Security awareness training is provided to staff at their induction and at regular intervals, as well as to contractors and consultants before they can access data and information.
- Maintenance of a Designated Security Assessed Position Register which details the IHPA staff and representatives which have been granted a security clearance by the Australian Government Security Vetting Agency.
- Establishment of an Audit, Risk and Compliance Committee that meets regularly to discuss issues, with a Chairperson independent to IHPA.
- Arranging regular internal and external security audits of its operations.
- Regular compliance reporting to the CEO, Pricing Authority and internal committees.

3.2 Assurance

IHPA has active processes to assess the effectiveness of internal controls. IHPA undertakes regular monitoring of compliance through the following:

- 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 PSPF 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
Twitter @IHPAnews

www.ihpa.gov.au

IHPA