Ownership:	Document Code:	Total Pages:
DEPARTMENT OF POLICY AND PLANNING	DPP/CDGG/V.3/06/2025	16
		Version: 3
Title: MINISTRY OF HEALTH DATA HANDLING AND SECURITY GUIDELINES FOR CONTRACTORS: *GUIDING ALL EXTERNAL PARTIES IN SAFEGUARDING THE PRIVACY, SECURITY, AND INTEGRITY OF MOH DATA*		Date of Issue: 08/11/2025
		Date of Next Review: 08/11/2028

TABLE OF CONTENTS:

Ownership:	Document Code:	Total Pages:
DEPARTMENT OF POLICY AND PLANNING	**DPP/CDGG/V.3/06/2025**	**16**
		Version: **3**
Title: **MINISTRY OF HEALTH DATA HANDLING AND SECURITY GUIDELINES FOR CONTRACTORS: *GUIDING ALL EXTERNAL PARTIES IN SAFEGUARDING THE PRIVACY, SECURITY, AND INTEGRITY OF MOH DATA***		**Date of Issue:** **08/11/2025**
		Date of Next Review: **08/11/2028**

1. BACKGROUND

1.1 The Ministry of Health (MOH) of Brunei Darussalam is committed to ensuring the highest standards of data governance across all its operations, including those involving contractors. This document outlines comprehensive guidelines that all contractors must adhere to when handling MOH data. These guidelines are designed to protect the privacy, security, and integrity of all data under MOH's purview, particularly sensitive healthcare information, and to ensure compliance with the Personal Data Protection Order (PDPO) of Brunei Darussalam.

2. PURPOSE

2.1 The purpose of these guidelines is to guide contractors in securely handling MOH data, protecting the privacy, security, and integrity of all data under MOH's purview, particularly sensitive healthcare information, and to ensure compliance with the PDPO of Brunei Darussalam.

3. SCOPE

3.1 These guidelines shall apply to all contractors who handle or have access to organisational data. It includes contractors who may be involved in processing, managing, or storing data on behalf of the organisation. The policy is applicable to all data, regardless of its classification, within the scope of their engagement.

4. DEFINITION

4.1 Public Data

4.1.1 Information freely available to the public requiring minimal protection.

4.2 Controlled Data

4.2.1 Non-public data with restricted access.

4.3 Restricted Data

4.3.1 Sensitive information requiring strict access controls

4.4 Confidential Data

4.4.1 Highly sensitive information requiring the highest level of protection

4.5 Personal Data

4.5.1 Any data, whether true or not, about an individual who can be identified from that data, or from that data and other information to which the organisation has or is likely to have access.

4.6 Data Breach

4.6.1 Any unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction of personal data.

4.7 Data Lifecycle

4.7.1 The entire process of data management, from collection to destruction, including creation, storage, use, sharing, archiving, and disposal.

4.8 Metadata

4.8.1 Data that provides information about other data, facilitating the understanding, use, and management of data.

5. ROLES AND RESPONSIBILITIES

5.1 Data Protection Officer (DPO)

5.1.1 Cooperate fully with MOH's DPO in all matters related to personal data protection.

5.1.2 Promptly report any personal data breaches or potential risks to the DPO.

5.1.3 Assist the DPO in conducting Data Protection Impact Assessments (DPIAs) when required.

5.1.4 Provide all necessary information to the DPO to demonstrate compliance with data protection regulations and this policy.

5.2 IT Security Officer (ITSO)

5.2.1 Adhere to all security protocols and standards set by MOH's ITSO.

5.2.2 Promptly report any security incidents or vulnerabilities to the ITSO.

5.2.3 Cooperate with the ITSO in implementing and maintaining security controls.

5.2.4 Participate in security assessments and provide all necessary information as requested by the ITSO.

5.3 Chief Ethics Officer (CethO)

5.3.1 Adhere to ethical guidelines set forth by MOH's CethO in all data-related activities.

5.3.2 Consult with the CethO on any ethical concerns or dilemmas related to data use.

5.3.3 Participate in ethics training programs as directed by the CethO.

5.4 Chief Medical Informatics Officer (CMIO)

5.4.1 Align data management practices with clinical informatics standards set by the CMIO.

5.4.2 Consult with the CMIO on matters related to health data standards and interoperability.

5.4.3 Provide feedback on the usability and effectiveness of clinical data systems.

6. PROCEDURES

6.1 Data Classification and Handling - MOH classifies data into four levels, each requiring specific handling procedures:

6.1.1 Public Data

6.1.1.1 Handling: Can be stored on public servers with minimal access control.

6.1.1.2 Examples: Public health statistics, general health education materials.

6.1.2 Controlled Data

6.1.2.1 Handling: Store on secure servers with access controls, conduct regular audits.

6.1.2.2 Examples: Internal communications, operational data, staff directories.

6.1.3 Restricted Data

6.1.3.1 Handling: Encrypt data both at rest and in transit.

6.1.3.2 Handling: Restrict access to authorized healthcare professionals only.

6.1.3.3 Handling: Conduct regular security reviews and audits.

6.1.3.4 Examples: Patient identifiers, medical records, treatment plans.

6.1.4 Confidential Data

6.1.4.1 Handling: Use strong encryption methods for data at rest and in transit.

6.1.4.2 Handling: Implement multi-factor authentication for access.

6.1.4.3 Handling: Maintain detailed logging and continuous monitoring of access attempts and usage.

6.1.4.4 Handling: Store in highly secure environments with stringent physical security controls.

6.1.4.5 Examples: Genetic information, mental health records, information related to high-risk conditions.

6.2 Security Controls

6.2.1 Access Control

6.2.1.1 Implement role-based access control for all systems handling MOH data.

6.2.1.2 Use multi-factor authentication for access to restricted and confidential data.

6.2.1.3 Regularly review and update access privileges.

6.2.1.4 Maintain detailed logs of all access to MOH data.

6.2.2 Encryption

6.2.2.1 Encrypt all confidential and restricted data at rest and in transit.

6.2.2.2 Use industry-standard encryption algorithms and key management practices.

6.2.2.3 Regularly review and update encryption methods to ensure they remain secure.

6.2.3 Physical Security

6.2.3.1 Secure physical access to any devices or areas where MOH data is processed or stored.

6.2.3.2 Implement surveillance and access logging for sensitive areas.

6.2.3.3 Ensure proper disposal of physical documents containing MOH data (e.g., using cross-cut shredders).

6.2.4 Network Security

- **6.2.4.1** Implement firewalls, intrusion detection/prevention systems, and regular vulnerability scans.
- **6.2.4.2** Segment networks to isolate systems handling sensitive MOH data.
- **6.2.4.3** Regularly patch and update all systems and software.

6.2.5 Mobile Device and Remote Access

- **6.2.5.1** Enforce encryption and remote wipe capabilities on all mobile devices accessing MOH data.
- **6.2.5.2** Use secure VPN connections for remote access to MOH systems.

6.3 Data Quality Management

6.3.1 Maintain data quality across the following dimensions:

- **6.3.1.1** Accuracy: Ensure data is correct, precise, and free from errors.
- **6.3.1.2** Completeness: All required data elements must be present.
- **6.3.1.3** Consistency: Data must be consistent within and across systems.
- **6.3.1.4** Timeliness: Data must be up to date and available when needed.
- **6.3.1.5** Validity: Data must comply with relevant rules and definitions.

6.3.2 Implement automated data validation checks to identify and flag potential quality issues.

6.3.3 Establish processes for regular data cleansing and error correction.

6.3.4 Conduct periodic data quality audits and report results to MOH.

6.3.5 Implement master data management practices to ensure consistency of key data entities across systems.

6.4 Data Lifecycle Management

6.4.1 Data Collection

- **6.4.1.1** Only collect data for specific, legitimate purposes as defined by MOH.
- **6.4.1.2** Ensure proper consent is obtained where required.

6.4.1.3 Use secure collection methods to protect data integrity and confidentiality.

6.4.2 Data Storage

6.4.2.1 Store data in secure, resilient systems with appropriate access controls.

6.4.2.2 Implement regular backup procedures and test data recovery processes.

6.4.2.3 Adhere to MOH's data retention policies.

6.4.3 Data Use

6.4.3.1 Use data only for the purposes for which it was originally collected.

6.4.3.2 Implement monitoring systems to detect potential misuse of data.

6.4.4 Data Sharing

6.4.4.1 Any MOH data must not be shared with third parties without explicit written authorization.

6.4.4.2 All data sharing must be governed by formal data sharing agreements approved by MOH.

6.4.4.3 Use secure methods for any authorized data transfers.

6.4.5 Data Archival

6.4.5.1 Securely archive data no longer in active use but required for retention.

6.4.5.2 Ensure archived data remains accessible and usable when needed.

6.4.5.3 Maintain metadata for archived data to facilitate future understanding and use.

6.4.6 Data Destruction (Appendix A)

6.4.6.1 Securely and permanently destroy data at the end of its lifecycle.

6.4.6.2 Use appropriate methods such as secure overwriting, degaussing, or physical destruction.

6.4.6.3 Provide certificates of destruction to MOH when required.

6.5 Metadata Management

6.5.1 Adhere to MOH's metadata standards for all data assets handled.

6.5.2 Ensure metadata accurately describes the content, structure, and context of data assets.

6.5.3 Required metadata elements may include: title, description, data owner, update frequency, access restrictions, and data quality metrics.

6.5.4 Capture metadata at the time of data creation and update it when significant changes occur.

6.5.5 Participate in MOH's data cataloging efforts as required.

6.6 Data Architecture and Integration

6.6.1 Data Architecture

6.6.1.1 Align with MOH's enterprise data model and architecture standards.

6.6.1.2 Design and maintain data architecture that supports MOH's integration and interoperability goals.

6.6.1.3 Regularly review and update data architecture to ensure alignment with evolving business needs and system changes.

6.6.1.4 Document all data architecture decisions and maintain up-to-date architectural diagrams.

6.6.2 Data Integration

6.6.2.1 Establish and maintain secure data integration processes that enable efficient and secure data exchange with MOH systems.

6.6.2.2 Use standardized data formats and protocols to minimize complexity and ensure interoperability.

6.6.2.3 Implement appropriate security controls for data in transit, including encryption and access authentication.

6.6.2.4 Maintain detailed documentation of all integration points and data flows.

6.6.3 Interoperability

6.6.3.1 All systems developed, managed, or maintained must support interoperability with MOH systems.

6.6.3.2 Implement support for internationally recognized open standards, particularly:

6.6.3.2.1 Health Level 7 (HL7)

6.6.3.2.2 Fast Healthcare Interoperability Resources (FHIR)

6.6.3.3 For systems with limited or no HL7/FHIR compatibility:

6.6.3.3.1 Provide and maintain appropriate middleware or integration platforms to ensure interoperability with MOH's fully HL7 and FHIR compatible systems.

6.6.3.3.2 Develop and implement a roadmap for achieving full HL7 and FHIR compatibility within an agreed timeframe.

6.6.3.3.3 Regular assessment and reporting of progress towards full compatibility.

6.6.4 Integration Testing and Validation

6.6.4.1 Conduct regular testing of all integration points and interoperability features.

6.6.4.2 Participate in MOH's integration testing initiatives as required.

6.6.4.3 Maintain test environments that accurately reflect production configurations.

6.6.4.4 Document and address any integration or interoperability issues promptly.

6.7 Personal Data Protection and Privacy

6.7.3 Consent

6.7.3.1 Ensure valid consent is obtained before collecting, using, or disclosing personal data, unless an exception applies.

6.7.3.2 Consent must be specific, informed, and clearly communicated.

6.7.3.3 Maintain records of all consent obtained.

6.7.4 Purpose Limitation

6.7.4.1 Collect, use, or disclose personal data only for purposes that a reasonable person would consider appropriate in the circumstances.

6.7.4.2 Do not use personal data for new purposes without obtaining fresh consent.

6.7.5 Notification

6.7.5.1 Inform individuals of the purposes for collecting, using, or disclosing their personal data on or before such collection, use, or disclosure.

6.7.6 Access and Correction

6.7.6.1 Provide individuals with access to their personal data upon request.

6.7.6.2 Allow individuals to correct errors or omissions in their personal data.

6.7.6.3 Implement procedures to handle access and correction requests promptly.

6.7.7 Accuracy

6.7.7.1 Make reasonable efforts to ensure that personal data collected is accurate and complete, especially if it will be used to make decisions affecting the individual.

6.7.8 Protection

6.7.8.1 Implement reasonable security arrangements to protect personal data from unauthorized access, collection, use, disclosure, copying, modification, disposal, or similar risks.

6.7.9 Retention Limitation

6.7.9.1 Retain personal data only as long as necessary for legal or business purposes.

6.7.9.2 Establish a retention schedule for different types of personal data.

6.7.9.3 Securely dispose of personal data that is no longer needed.

6.7.10 Transfer Limitation

6.7.10.1 Do not transfer personal data out of Brunei Darussalam except in accordance with PDPO requirements.

6.7.10.2 Ensure that the overseas recipient is bound by legally enforceable obligations to provide a standard of protection comparable to that under the PDPO.

6.7.11 Data Breach Notification

6.7.11.1 Notify MOH of any data breaches that meet the PDPO's notification criteria.

6.7.11.2 Assist MOH in assessing if a data breach is notifiable under the PDPO.

6.7.12 Accountability

6.7.12.1 Develop and implement policies and practices necessary to meet PDPO obligations.

6.7.12.2 Make information about these policies and practices available upon request.

6.7.13 Do Not Call Provisions

6.7.13.1 Comply with any Do Not Call provisions that may be included in the PDPO, including checking relevant Do Not Call registries before sending marketing messages.

6.7.14 Data Protection Impact Assessments (DPIAs)

6.7.14.1 Conduct DPIAs for new high-risk processing activities or significant changes to existing processes.

6.7.14.2 Share DPIA results with MOH and implement recommended mitigation measures.

6.7.15 Privacy by Design

6.7.15.1 Incorporate data protection considerations into the design and operation of all systems, processes, and products that involve personal data.

6.7.16 Rights of Data Subjects

6.7.16.1 Respect and facilitate the exercise of data subject rights as defined in the PDPO, including the right to withdraw consent.

6.7.17 Data Portability

6.7.17.1 If included in the PDPO, be prepared to comply with data portability requirements, allowing individuals to receive their personal data in a commonly used machine-readable format.

6.8 Incident Reporting and Breach Management

6.8.1 Report any suspected or confirmed data breaches to MOH's designated contact immediately, and no later than 24 hours after discovery.

6.8.2 Provide all relevant information about the breach, including:
- **6.8.2.1** Date and circumstances of the breach
- **6.8.2.2** Nature and extent of the personal data involved
- **6.8.2.3** Potential consequences of the breach
- **6.8.2.4** Measures taken or proposed to address the breach

6.8.3 Cooperate fully with MOH in any breach investigation and mitigation efforts.

6.8.4 Maintain an integral breach register and contribute to lessons learned processes.

6.9 Training and Awareness

6.9.1 Ensure all staff handling MOH data receive comprehensive initial training on these guidelines and data protection principles.

6.9.2 Conduct regular refresher training, at least annually.

6.9.3 Maintain training records and provide them to MOH upon request.

6.10 Compliance and Audit

6.10.1 Maintain detailed documentation of all data processing activities performed on behalf of MOH.

6.10.2 Conduct regular internal audits to ensure compliance with these guidelines.

6.10.3 Cooperate fully with any audits or inspections conducted by MOH or its authorized representatives.

6.10.4 Implement prompt corrective actions for any identified non-compliance issues.

6.11 Continuous Improvement

6.11.1 Regularly review and update data governance practices to ensure ongoing compliance and effectiveness.

6.11.2 Participate in MOH's data governance improvement initiatives as required.

6.11.3 Provide feedback on data governance processes and suggest improvement where applicable.

6.11.4 Stay informed about evolving data protection laws and best practices, and implement changes as needed.

6.12 Ethical Considerations

6.12.1 Adhere to ethical principles in all data handling activities, including respect for individual privacy and autonomy.

6.12.2 Consider potential impacts on individuals and communities when processing sensitive health data.

6.12.3 Raise any ethical concerns about data use to MOH's ethics committee.

6.13 Termination

6.13.1 Upon termination of contract, return or securely destroy all MOH data as instructed.

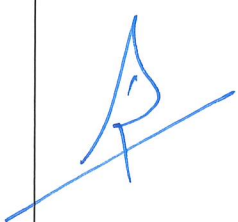
6.13.2 Provide written certification of data destruction when applicable.

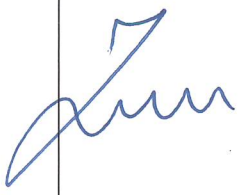
6.13.3 Ensure that no MOH data is retained unless explicitly authorized for specific, documented purposes.

7 REFERENCES

7.1 Literatures, websites, book titles, and material used in formulating the content of the document, using American Psychologists Association (APA) format as basic referencing style.

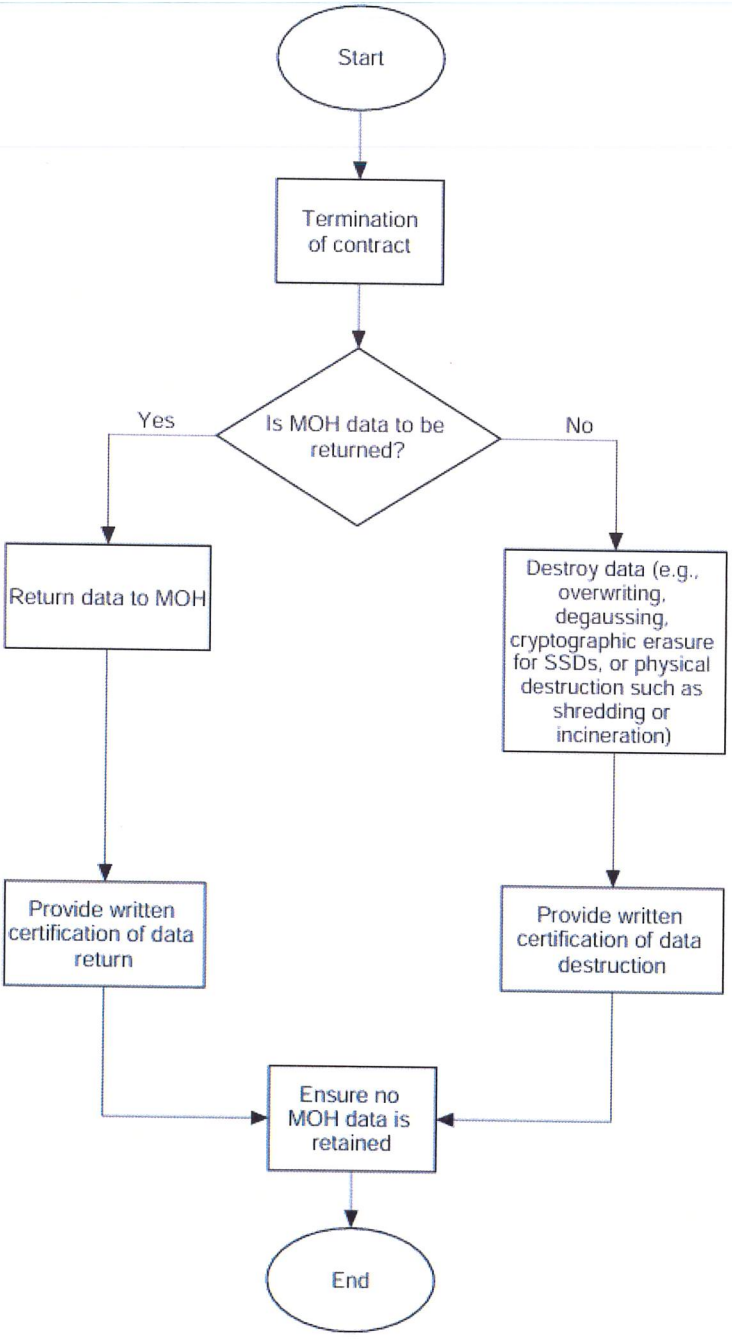
ACKNOWLEDGEMENT

ACTION	NAME & DESIGNATION	SIGNATURE	DATE
Authored/ Revised by:	Haji Adi Ihram bin Dato Paduka Haji Mahmud, Director Department of Policy and Planning		20/11/2025
Reviewed by:	Pg Dr Noor Azmi Pg Dr Hj Mohammad, Chief Medical Informatics Officer Consultant Orthopaedic Surgeon Digital Health Unit, MOH RIPAS Hospital		10.1.26

	Department of Orthopaedic Surgery RIPAS Hospital		
	Dr Hj Zulhilmi POKHPDSS Hj Abdullah, Chief Medical Informatics Officer Consultant Primary Health Care Digital Health Unit, MOH		10/01/2026
	Rudy Hj Harun, Director of Healthcare Technology, Healthcare Technology Department, MOH		05/02/26
	Dr Alice Yong Moi Ling, Chair of Bioethics, Biomedical Research and Ethics Unit, MOH Consultant Endocrinologist Biomedical Research and Ethics Unit, MOH Endocrine Centre, RIPAS Hospital Department of Internal Medicine		16.12.2025
Endorsed by:	Yang Mulia Dr Hajah Rafidah binti Haji Gharif, Deputy Permanent Secretary.		12.2.26
Contributed by:	Muhammad Nur Hafizuddin bin Haji Hamidi, Apprentice.		

Ownership:	Document Code:	Total Pages:
DEPARTMENT OF POLICY AND PLANNING	**DPP/CDGG/V.3/06/2025**	**16**
		Version: **3**
Title: **MINISTRY OF HEALTH DATA HANDLING AND SECURITY GUIDELINES FOR CONTRACTORS: *GUIDING ALL EXTERNAL PARTIES IN SAFEGUARDING THE PRIVACY, SECURITY, AND INTEGRITY OF MOH DATA***		**Date of Issue:** **08/11/2025**
		Date of Next Review: **08/11/2028**

APPENDICES (if applicable)
Appendix A: Data Destruction


Start
Termination of contract
Is MOH data to be returned?
Yes
No
Return data to MOH
Destroy data (e.g., overwriting, degaussing, cryptographic erasure for SSDs, or physical destruction such as shredding or incineration)
Provide written certification of data return
Provide written certification of data destruction
Ensure no MOH data is retained
End

<table>
<tr><td>Ownership:

DEPARTMENT OF POLICY AND PLANNING</td><td>Document Code:

DPP/CDGG/V.3/06/2025</td><td>Total Pages:

16</td></tr>
<tr><td colspan="2" rowspan="2">Title:

MINISTRY OF HEALTH DATA HANDLING AND SECURITY GUIDELINES FOR CONTRACTORS: GUIDING ALL EXTERNAL PARTIES IN SAFEGUARDING THE PRIVACY, SECURITY, AND INTEGRITY OF MOH DATA</td><td>Version:

3</td></tr>
<tr><td>Date of Issue:

08/11/2025</td></tr>
<tr><td colspan="2"></td><td>Date of Next Review:

08/11/2028</td></tr>
</table>

ANNEXES (if applicable)
Is considered as supporting documents and shall not have page number(s) that are in continuation with that particular document.