PURECS

Data Privacy and Protection Policy

Document Classification	Internal
Document ref	Data Privacy and Protection Policy v2.0
Policy Owner	Information Security & Technology GRC
Implementation Owner	Information Security & Technology GRC

Revision history

VERSION	DATE	SUMMARY OF CHANGES
1.0	22nd Nov 2023	First release
2.0	6th Dec 2024	• Addition of relevant regulations • Logo changes • General content improvements

Author

NAME	DESIGNATION	SIGNATURE
Giridhar Govindarajan	Manager – IT Governance	

Reviewed by

NAME	DESIGNATION	SIGNATURE
Syed Shoaib Hasan	Director – Information Security & Technology Governance Risk and Compliance	

Approved by

NAME	DESIGNATION	SIGNATURE
Junaid Khan	Chief Executive Officer	

Table of Contents

1. Introduction

This policy serves as foundational document that outlines the standards, principles, guidelines, processes, and procedures governing the responsible handling of information within PureCS. It is designed to ensure compliance with legal and regulatory requirements and establish a culture of trust and transparency among stakeholders, including employees, and customers.

This policy recognizes the inherent value of information as a strategic asset and emphasizes the commitment to preserving the privacy of data. It addresses all sensitive & non-sensitive information (including but not limited to PII, PHI & confidential information) acknowledging the unique considerations each type entails.

2. Purpose

The purpose of this policy is to ensure all sensitive & non-sensitive information (including but not limited to PII, PHI & confidential information) is protected from unauthorized access, use, modification or disclosure in compliance with local UAE laws, ministerial decrees and regulatory obligations mandated by health authorities & Central Bank of UAE.

3. Scope

This scope covers all sensitive & non-sensitive information (including but not limited to PII, PHI & confidential information) handled, managed or owned by PureCS in its provision of technology services & solutions.

4. Responsibilities

Group	Responsibility
Information Security and Technology - Governance, Risk & Compliance	• Development, maintenance, and enforcement of the policy • Conduct user awareness • Monitor compliance with this policy
Executive Management	• Endorsement of this policy
HR	• Handle disciplinary actions for policy non-compliance
Users	• Read, understand, and adhere to this policy

Group	Responsibility
IT Security and Infrastructure	• Support business units in implementation of the defined controls in this policy

5. References

1. Clean desk and Clear Screen Policy
2. Identity and Access Management Policy
3. Secure Information Exchange Policy
4. Information Classification, Labelling, and Handling Policy
5. Asset Management Policy
6. Incident Management Policy
7. Exception Policy
8. Data Privacy & Protection Standard
9. ADHICS
10. Department of Health (DOH)
11. Dubai Health Authority (DHA)
12. Ministry of Health and Prevention (MoHAP)
13. Group Data Privacy & Protection Policy
14. Central Bank of UAE

6. Definition

Group	Definition
Information Asset	Any technology or non-technology resource that holds, processes, or transmits corporate information shall be considered as information asset. It shall include but not limited to: • Hardware (ex: laptop, screens, servers etc). • Software (ex: applications, operating systems, etc). • Human Resources
Users	Includes all employees, interns, temporary staff, contractors, third parties or any other personnel who have been provisioned access to PHG owned/managed assets.

Group	Definition
Personally Identifiable Information (PII)	PII refers to any information that can be used to identify a specific individual, either on its own or when combined with other information.
Protected Health Information (PHI)	PHI refers to any information in a medical context that can be used to identify an individual and is related to their physical or mental health condition, the provision of healthcare, or payment for healthcare services.
Data / Information	In this document, the terms "data" and "information" are used interchangeably to refer to any collected or processed facts, figures, and insights. Both terms signify the essential elements that contribute to knowledge and decision-making processes.
Data Controller	A data controller is an entity (person, company, organization) that determines the purposes and means of processing personal data. In other words, the data controller decides how and why personal data is processed.
Data Processor	A data processor is an entity (person, company, organization) that processes personal data on behalf of the data controller. The data processor does not determine the purposes and means of the processing but acts on the instructions of the data controller.

7. Principles

7.1. The Privacy Rule

1. Protects an individual's PHI
2. Identifies permitted users and disclosures of PHI
3. Gives patients control over their PHI (Patient' Rights)

7.2. The Security Rule

1. Protects and individual's health care information that is maintained or transmitted electronically

2. Defines administrative, physical, and technical safeguards for electronic PHI (ePHI)
3. Requires corrective action for workforce members who fail to comply with policies and procedures

7.3. The Breach Notification Rule

1. Requires that a breach of PHI be reported unless it can be demonstrated "that there is a low probability that the PHI has been compromised based on a risk assessment" of certain factors.

8. Policy Statements

1. PureCS shall identify and meet the requirements regarding the preservation and protection of all sensitive & non-sensitive information (including but not limited to PII, PHI & confidential information) according to applicable laws, regulations and contractual requirements.
2. This policy shall be communicated to all users including but not limited to, data controller and data processor involved in processing of sensitive & non-sensitive information (including but not limited to PII, PHI & confidential information).
3. Information/data shall be suitably protected by adequate means and methods.
4. Data privacy and protection shall be considered in design of systems and applications.
5. A data privacy notice[1] shall be established
6. Technical, physical and administrative controls shall be applied to protect all data in accordance with data privacy requirements mandated by, but not limited to MOHAP, DOH, DHA, and CBUAE.
7. A combination of user awareness and strict implementation of policies and procedures shall be implemented to protect data privacy.
8. Periodic risk assessment shall be conducted to identify and address data privacy risks.
9. Relevant regulatory authority shall be notified in the event of a data breach.
10. Awareness on data protection and privacy shall be conducted for all employees

[1] Refer Appendix: Data Privacy Notice

11. Clean desk and clear screen[2] practice shall be strictly enforced and adhered in areas where sensitive information (including but not limited to PII, PHI & confidential information) accessed, stored, handled, or processed.
12. Access to sensitive information (including but not limited to PII, PHI & confidential information) shall be strictly controlled.
13. Access criteria to all sensitive (including but not limited to PII, PHI & confidential information) shall be defined and enforced[3].
14. Relevant restrictions on printing and sharing of information shall be enforced[4].
15. Hardcopy/media containing sensitive information (including but not limited to PII, PHI & confidential information) shall be securely stored or shredded after use[5].
16. The purpose for which data is collected before initiating any data collection process shall be clearly defined
17. It shall be ensured that the data collected is directly relevant and necessary to achieve the specified purpose.
18. A privacy notice shall be published for end users.
19. Collection of data shall be limited to what is adequate, relevant, and necessary in relation to the purposes for which it is processed.
20. Collecting excessive or unnecessary data shall be avoided
21. Periodic review of data collection practices shall be conducted to ensure only necessary information is collected
22. Data collection forms and processes shall be periodically updated to remove any fields that are not essential.
23. Cross-border data transfer shall be restricted unless compliant with regulatory requirements.
24. There shall be a legitimate use case and required approvals from relevant authorities before data is transferred cross-border.
25. Data shall be protected using suitable techniques during transfers.
26. Upon detecting a data breach, immediate steps shall be taken to contain and mitigate the breach to prevent further unauthorized access or damage.

[2] Refer Clean desk and Clear Screen Policy
[3] Refer Identity and Access Management Policy
[4] Refer Secure Information Exchange Policy
[5] Refer Asset Management Policy

27. The nature and extent of the breach shall be assessed, including the types of data involved, the potential impact on individuals, and the likelihood of harm.
28. If the data breach is likely to result in a risk to the rights and freedoms of individuals, relevant data protection authorities, regulatory bodies and affected users shall be notified without undue delay and, where feasible, within reasonable time of becoming aware of the breach.

9. Incident Reporting

Incidents related to this policy shall be reported to service desk[6].

10. Policy Compliance

1. Requirements of this policy and supporting policies will be enforced by designated functions on the direction of PHG and/or PureCS's management
2. Non-compliance to these policies will be addressed as per Code of Conduct and HR Manual
3. If users are unsure or not clear of anything in this policy, they should seek clarification or advice from IST Governance Risk and Compliance function
4. IST Governance Risk and Compliance reserves the right to check the compliance of this policy on a periodic basis
5. Any exceptions to this policy shall follow a formal exception request process. Exception can also be provisioned to nominated functions/departments as directed by Executive Management

[6] Refer Incident Management Policy