شركة البحيرة الوطنية للتأمين
Al-Buhaira National Insurance Co.

Data Privacy Policy

Document Control

Approved by	Position	Date	Signature
Mr. Issam Mehdawi	Acting CEO		
Mr. Nabil Shanawani	Head of ITISMC		
Mr. Salah F. Daou	ITISMC Member		
Mr. Ayed Saleh	ITISMC Member		
Mr. Mohammed Rashid Ali	ITISMC Member		

Document Review and Version Control			
Review Cycle	**1 Years**	**Next Review Date**	**31-DEC-2026**

Doc Ref	Version No.	Revision Description	Classification	Doc Author	Doc Owner	Revision Date
ISMS-200126	V1.0	Initial Draft	Restricted	Security Engineer	ITISMC	20/01/2026
ISMS-200126	V1.1	Change	Restricted	Security Engineer	ITISMC	22/01/2026
ISMS-200126	V1.2	Change	Restricted	Security Engineer	ITISMC	15/05/2026

Draft Verification				
Name	**Designation**	**Section Updated**	**Signature**	**Date of Verification**
Md Tausif Reza	Security Engineer	Review		20/01/2026
Md Tausif Reza	Security Engineer	Roles and Responsibilities		22/01/2026
Md Tausif Reza	Security Engineer	Remediation of Findings of V1.1		15/05/2026

Table of Contents

1 Purpose

This Data Privacy Policy establishes the principles, responsibilities and controls required to ensure the lawful, fair, transparent and secure processing of personal data, patient identifiable information and protected health information handled by the organization. This policy supports protection of personal and health information against unauthorized access, misuse, unlawful disclosure, alteration, loss or destruction.

2 Scope

This policy applies to:

- All personal data relating to patients, employees, contractors, visitors, vendors and other third parties.
- All sensitive personal data and health information processed, stored, transmitted or disposed of by the organization.
- All processing activities across clinical systems, EMR/EHR platforms, administrative systems, cloud services, mobile devices, endpoint devices, network services, backup systems and paper records.
- All personnel, including permanent employees, temporary employees, contractors, healthcare professionals, interns, consultants and approved third parties with authorized access.
- All stages of the data lifecycle, including collection, use, storage, transfer, sharing, retention, archival, anonymization and secure deletion.

3 Regulatory and Standards References

This policy shall be applied in line with applicable legal, regulatory, contractual and sector-specific privacy and information security requirements, including:

- UAE Personal Data Protection Law (PDPL) and applicable implementing regulations.
- ADHICS (Abu Dhabi Healthcare Information and Cyber Security Standard), where applicable to the organization.
- ISO/IEC 27001:2022 for information security management.
- ISO/IEC 27701 for privacy information management.
- NESA UAE Information Assurance Regulation, where applicable.
- Applicable healthcare privacy regulations, licensing requirements and contractual obligations.

Where this policy conflicts with applicable law or regulator instructions, the stricter legal or regulatory requirement shall prevail.

4 Definitions

Term	Definition
Personal Data	Any information relating to an identified or identifiable natural person.
Sensitive Personal Data	Personal data requiring additional protection, including health data, biometric data, genetic data, identification documents and other categories defined by applicable law.

Term	Definition
Patient Identifiable Information (PII)	Information that can identify a patient directly or indirectly, including name, ID number, medical record number, contact details or other identifiers.
Protected Health Information (PHI)	Health-related information linked to an identifiable individual.
Data Subject	The individual to whom personal data relates.
Processing	Any operation performed on personal data, including collection, recording, storage, use, disclosure, transfer, restriction, deletion or destruction.
Consent	A clear, informed, specific and freely given indication by which a data subject agrees to the processing of personal data for defined purposes.
Data Controller	The entity that determines the purposes and means of processing personal data.
Data Processor	A party that processes personal data on behalf of the controller under documented instructions.
Data Protection Officer (DPO)	The appointed person responsible for advising, monitoring, coordinating and supporting compliance with privacy and data protection requirements.
Data Breach / Privacy Incident	A security or privacy event leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data.
Cross-Border Transfer	Transfer, storage, remote access or processing of personal data outside the country or approved jurisdiction.
Anonymization	Irreversible processing that prevents identification of the data subject.
Pseudonymization	Processing that reduces identifiability by replacing identifiers with codes or tokens while keeping separate re-identification information secured.

5 Privacy Governance and Accountability

The organization shall maintain a privacy governance structure to ensure accountability for the processing of personal and health information

5.1 Management Accountability

- Senior management shall approve this policy and ensure adequate resources are available to implement privacy controls.
- Management shall ensure that privacy risks are reported through the appropriate governance forum.
- Policy exceptions shall require documented risk acceptance and management approval.

5.2 Data Protection Officer

- The organization shall appoint a Data Protection Officer or designated privacy lead with sufficient authority and independence to oversee privacy compliance.
- The DPO shall advise the organization on privacy obligations, review privacy notices, support data subject requests, monitor policy implementation, and coordinate breach notification assessment.
- The DPO shall maintain a privacy risk register, data subject request register, consent register, transfer register and breach register as applicable.
- The DPO shall be consulted for new projects, high-risk processing, cross-border transfers, third-party processing and privacy incidents.

5.3 Records of Processing Activities

- Data owners, with support from the DPO and Information Security Team, shall maintain records of processing activities for systems and processes involving personal data.
- The record shall identify the processing purpose, categories of data, lawful basis, data subjects, data recipients, retention period, location, transfers and security controls.
- Processing records shall be reviewed at least annually or when a major process, system or third-party relationship changes.

6 Privacy Principles

The organization shall process personal and health data according to the following principles.

6.1 Lawfulness, Fairness and Transparency

Personal data shall be processed only when a lawful basis exists, and the processing is fair, transparent and consistent with the information provided to the data subject through privacy notices or consent statements.

6.2 Collection and Purpose Limitation

Personal data shall be collected only for explicit, specified and legitimate purposes. Data shall not be used for purposes that are incompatible with the original purpose unless a valid lawful basis exists, consent is obtained where required, or the new purpose is otherwise permitted by applicable law.

6.3 Data Minimization and Accuracy

Only the minimum personal data necessary for the defined purpose shall be collected and processed. Reasonable steps shall be taken to keep personal and health information accurate, complete, relevant and up to date.

6.4 Storage Limitation

Personal data shall be retained only for the period required by healthcare, legal, regulatory, contractual or business requirements. After the retention period expires, the data shall be securely deleted, anonymized or archived under controlled conditions.

6.5 Integrity, Confidentiality and Security

Appropriate technical and organizational controls shall protect data from unauthorized access, accidental loss, unlawful disclosure, alteration or destruction. Controls shall include access management, encryption, logging, monitoring, network security, secure configuration and incident response.

6.6 Accountability

The organization shall be able to demonstrate compliance with this policy through documented approvals, registers, logs, training records, audit results, risk assessments and management review evidence.

7 Lawful Basis for Processing

Personal and health data shall be processed only where at least one lawful basis applies. The lawful basis shall be documented before processing begins and reviewed when the processing purpose changes.

- Provision of healthcare services and continuity of care.
- Compliance with legal, regulatory, licensing or public health obligations.
- Patient safety, emergency care, public health or vital interest requirements.
- Contractual necessity for employment, vendor, patient administration or service delivery.
- Explicit consent where required by law, policy or the nature of processing.
- Legitimate organizational purposes were permitted and balanced against data subject rights and expectations.

Data owners shall not rely on consent where another lawful basis is more appropriate, or where the data subject cannot freely refuse or withdraw consent without unfair consequences.

8 Consent Management

Consent shall be obtained, recorded and managed where required for the collection, use, disclosure or transfer of personal or sensitive personal data. Consent shall be specific to the purpose of processing and shall not be bundled with unrelated terms.

8.1 Consent Collection Requirements

- Consent requests shall clearly describe the purpose of processing, categories of data, parties who may receive the data, any cross-border transfer, retention period where possible, and the right to withdraw consent.
- Consent shall be captured through approved forms, digital workflows, signed declarations or other auditable methods.
- For sensitive personal data or health data, explicit consent shall be obtained where required unless another lawful basis or legal obligation applies.

- Consent shall be written in clear and understandable language and shall be available in the languages required by the organization and its data subjects.
- Consent for minors or legally incapable individuals shall be obtained from the parent, guardian or legally authorized representative where required.

8.2 Consent Records and Withdrawal

- The DPO or designated owner shall maintain a consent register or system record showing the data subject, date, method, purpose, version of notice/consent statement and scope of consent.
- Data subjects shall be able to withdraw consent through a clear process that is no more difficult than giving consent.
- Withdrawal of consent shall be logged and applied to future processing unless the organization must continue processing for legal, regulatory, healthcare or contractual reasons.
- Systems and teams shall be notified of consent withdrawal where processing must stop or be restricted.
- Consent statements and forms shall be reviewed periodically to ensure they remain accurate and aligned with current processing activities.

9 Privacy Notices and Transparency

The organization shall provide privacy notices before or at the time of data collection, unless an exception applies. Privacy notices shall be easy to access, clear and accurate.

- Privacy notices shall explain what data is collected, why it is collected, lawful basis, how it is used, who it may be shared with, whether it is transferred across borders, retention periods, data subject rights and DPO contact details.
- Website, portal, mobile application, patient registration and employee onboarding notices shall be aligned with this policy.
- Where processing changes materially, the privacy notice shall be updated and data subjects shall be informed where required.
- A current approved version of the privacy policy or public privacy notice shall be published on the organization website and internal portal.

10 Collection, Use and Purpose Limitation

Personal data shall be collected and used only for documented, legitimate and approved purposes. The organization shall avoid excessive or unnecessary data collection.

10.1 Collection Controls

- Each form, system or process collecting personal data shall identify the purpose, lawful basis, mandatory fields, optional fields and data owner.

- Data collection points shall be reviewed by the DPO, Legal/Compliance or Information Security Team for new or high-risk processing.
- Personal data shall not be collected from third-party sources unless the source is lawful, authorized and documented.
- Use of personal data for marketing, research, analytics, system testing or training shall require approval and appropriate safeguards such as consent, anonymization or pseudonymization where applicable.

10.2 Secondary Use

- Secondary use of data shall be assessed against the original purpose, data subject expectations, applicable law and privacy risk.
- Where secondary use is incompatible with the original purpose, processing shall not proceed unless a new lawful basis is documented and consent is obtained where required.
- Data owners shall ensure that changes in processing purpose are reflected in the processing record and privacy notice.

11 Data Subject Rights

The organization shall respect and facilitate the rights of data subjects in accordance with applicable law, healthcare regulations and contractual requirements.

11.1 Rights Supported by the Organization

- Right to be informed about collection and processing of personal data.
- Right of access to personal data held by the organization, subject to verification and lawful limitations.
- Right to correction or rectification of inaccurate or incomplete data.
- Right to deletion or erasure where applicable and where retention is not legally required.
- Right to restriction of processing where applicable.
- Right to object to processing where applicable.
- Right to data portability where applicable and technically feasible.
- Right to withdraw consent where processing is based on consent.
- Right to lodge a complaint with the organization or the relevant regulatory authority.

11.2 Data Subject Request Process

- Requests shall be submitted through approved channels such as the DPO email, patient relations, HR or designated portal.
- The identity and authority of the requester shall be verified before disclosure, correction, deletion or restriction action is taken.

- All requests shall be logged in a Data Subject Request Register, including request date, requester details, right exercised, assigned owner, due date, decision and closure evidence.
- Requests shall be assessed and answered within the timeframe required by applicable law or regulator instruction.
- If a request is denied or limited, the reason shall be documented and communicated where required.
- Data subject requests involving health records shall be handled with Clinical, Legal/Compliance and DPO involvement where required.

12 Retention, Archiving and Secure Deletion

The organization shall retain personal and health information only for the period necessary to fulfil the purpose of processing and to meet legal, regulatory, healthcare, contractual, audit and business requirements.

12.1 Retention Schedule

- Data owners shall maintain a retention schedule covering each record category, system, business process and legal basis for retention.
- Retention periods shall consider healthcare record retention requirements, employment requirements, finance requirements, litigation holds, regulatory audit obligations and contractual commitments.
- The retention schedule shall be reviewed at least annually and whenever legal or business requirements change.
- Data shall not be retained indefinitely unless there is a documented legal, regulatory or approved business justification.

12.2 Secure Deletion and Disposal

- After the retention period expires, data shall be securely deleted, destroyed or anonymized using approved methods.
- Electronic deletion shall use secure deletion procedures appropriate to the system, storage media and sensitivity of the information.
- Paper records shall be shredded or disposed of through approved confidential waste processes.
- Deletion activities shall be documented, including system/record category, approval, date, method and responsible person.
- Backups shall be protected and retained according to the backup retention schedule. Restored data that has expired shall be securely deleted again as soon as practicable unless legally required.

12.3 Legal Hold and Archiving

- Where litigation, investigation or regulatory requirement applies, deletion shall be suspended through a documented legal hold approved by Legal/Compliance.
- Archived data shall remain protected by access controls, encryption where applicable, monitoring and documented retrieval procedures.
- Archived data shall not be reused for new purposes without appropriate lawful basis, approvals and privacy assessment.

13 Access Control and Confidentiality

Access to personal and health data shall be granted based on the principle of least privilege, role-based access and need-to-know.

- Access shall be formally requested, approved by the data owner and provisioned by authorized IT personnel.
- Access rights shall be reviewed periodically and upon transfer, role change or termination.
- Privileged access shall be restricted, monitored, logged and reviewed.
- Shared or generic accounts shall not be used for accessing personal or health information unless approved as a controlled technical exception.
- All personnel and third parties shall sign confidentiality and acceptable use agreements before accessing information systems.
- Remote access shall use approved secure channels, strong authentication and monitoring.

14 Data Sharing, Third Party Processing and Disclosure

Personal and health data shall be shared only with authorized parties and only for lawful, documented and necessary purposes.

14.1 Internal and External Disclosure

- Internal disclosures shall be limited to personnel who need the information to perform authorized duties.
- External disclosures may include authorized healthcare providers, regulators, insurers, laboratories, auditors, service providers or other parties where lawful and necessary.
- Disclosures shall be documented where required, including recipient, purpose, data category, date and approval.
- Data shall not be shared through unauthorized channels such as personal email, unmanaged messaging applications or unapproved cloud services.

14.2 Third Party Processing Controls

- Third parties processing personal data shall undergo privacy and security due diligence before onboarding.

- Contracts shall include Data Processing Agreements, confidentiality clauses, permitted processing purposes, security requirements, breach notification obligations, audit rights, subcontracting restrictions, return/deletion obligations and cross-border transfer safeguards.
- Third-party access shall be reviewed periodically and terminated when no longer required.
- High-risk vendors shall be monitored through periodic reviews, security attestations, audits or compliance evidence.

15 Cross-Border Transfer of Personal Data

Cross-border transfer, storage, remote support access or processing of personal data outside the approved jurisdiction shall be controlled and shall not occur without documented assessment and approval.

15.1 Transfer Assessment and Approval

- Before cross-border transfer begins, the data owner shall complete a transfer assessment with support from the DPO, Legal/Compliance and Information Security Team.
- The assessment shall identify the data categories, purpose, destination country, recipient, onward transfer, hosting location, remote access arrangements, security controls and legal basis.
- Transfers shall require management approval and DPO/Compliance review before implementation.
- Regulator notification or approval shall be obtained where required by applicable law, healthcare regulation or contractual obligation.
- A Cross-Border Transfer Register shall be maintained and reviewed at least annually.

15.2 Transfer Safeguards

- Transfers shall be covered by appropriate contractual safeguards, including Data Processing Agreements and confidentiality obligations.
- Personal and health data shall be encrypted in transit and protected at rest where technically feasible and risk appropriate.
- Only the minimum necessary data shall be transferred and, where possible, data shall be anonymized or pseudonymized before transfer.
- Access by overseas support teams shall use approved remote access methods, multi-factor authentication, logging and time-bound access controls.
- Cloud hosting and backup locations shall be approved before use and documented in the asset and processing records.
- Cross-border transfer shall be suspended where the transfer risk becomes unacceptable or contractual/legal safeguards are no longer valid.

16 Data Breach and Privacy Incident Management

Actual or suspected personal data breaches and privacy incidents shall be reported, assessed, contained, investigated and remediated promptly according to the Incident Response Plan and this policy.

16.1 Reporting and Escalation

- All personnel shall immediately report suspected or confirmed privacy incidents to the Information Security Team, Service Desk, line manager or DPO through approved channels.
- Examples include lost devices, misdirected emails, unauthorized access, ransomware, accidental disclosure, excessive access, improper disposal, unauthorized transfer or suspected misuse of patient data.
- The Information Security Team shall notify the DPO, Legal/Compliance, affected data owners and management based on severity and impact.
- A breach register shall be maintained with incident details, timeline, impact assessment, actions taken, notification decision, root cause and closure evidence.

16.2 Assessment and Containment

- Incidents shall be triaged to determine whether personal data, sensitive data or health information is involved.
- Containment actions shall be implemented immediately to prevent further disclosure, loss or unauthorized access.
- The assessment shall consider type and volume of data, number of data subjects, sensitivity, likelihood of harm, system impact, third-party involvement and whether data was encrypted or otherwise protected.
- Evidence shall be preserved according to incident response and forensic requirements.

16.3 Notification and Remediation

- Regulators, affected individuals, customers, partners or other parties shall be notified where required by applicable law, healthcare regulation, contract or management decision.
- The DPO and Legal/Compliance shall support the decision on notification content, timing and recipients.
- Affected individuals shall be provided with clear information about the incident, data involved, possible risks, steps taken and recommended protective actions where notification is required.
- Root cause analysis shall be completed, and corrective actions shall be tracked to closure.
- Lessons learned shall be presented to the appropriate governance forum for high-risk or repeated incidents

17 Privacy by Design and Data Protection Impact Assessment

Privacy requirements shall be considered at the design stage of new systems, applications, processes, integrations, analytics initiatives and third-party services.

- Projects involving personal data shall complete a privacy screening before implementation.
- A Data Protection Impact Assessment (DPIA) shall be completed for high-risk processing, new technologies, large-scale health data processing, monitoring activities, cross-border transfers or processing that may significantly affect data subjects.
- DPIAs shall assess the purpose, necessity, proportionality, lawful basis, risks to data subjects, security controls, retention and third-party involvement.
- Security and privacy requirements shall be included in procurement, system development, change management and vendor onboarding processes.
- Testing and development environments shall not use real personal or health data unless approved and protected by appropriate controls

18 Awareness and Training

All personnel shall receive privacy and patient data protection training as part of onboarding and shall complete mandatory refresher training at least annually.

- Training shall cover privacy principles, ADHICS privacy obligations, patient confidentiality, secure handling of health data, phishing awareness, breach reporting, data subject rights, consent requirements and acceptable use of systems.
- Role-based training shall be provided for personnel with elevated privacy responsibilities, including DPO, data owners, IT administrators, HR, patient relations, clinical teams and employees handling sensitive data.
- Attendance shall be recorded and retained as evidence of compliance.
- Awareness communications shall be issued following major policy updates, incidents, regulatory changes or recurring audit findings.
- Staff awareness sessions shall be conducted as part of DP 1.1 remediation and evidence shall include attendance records, presentation material and communication screenshots.

19 Monitoring, Audit, Compliance and Enforcement

Compliance with this policy shall be monitored through internal audits, risk assessments, access reviews, system logs, privacy reviews, ADHICS compliance reviews and management reporting.

- Non-compliance with this policy may result in corrective action, disciplinary action, access revocation, contract termination or legal/regulatory consequences.
- Policy exceptions shall be documented, risk assessed, approved by authorized management and reviewed periodically.

- Privacy risks and significant findings shall be tracked in the risk register or corrective action register until closure.
- Internal Audit or the Compliance/ISMS Team may perform periodic assessments of privacy controls and evidence.

20 Publication and Communication

After approval, the current version of this policy shall be published and communicated to relevant stakeholders.

- The approved policy shall be published on the internal portal or document management system.
- A public-facing privacy notice or applicable privacy policy shall be published on the organization website where data is collected from patients, visitors, employees, vendors or other data subjects.
- Employees and relevant third parties shall be notified of the policy update through email, intranet announcement, awareness session or other approved communication method.
- Published copies shall be controlled to prevent use of outdated versions.
- Evidence of publication shall include internal portal screenshot, website screenshot, management approval and communication records.

21 Roles and Responsibilities

Role	Responsibility
Management / CEO	Approve the policy, provide resources, support privacy governance and approve high-risk exceptions where required.
ITISMC Committee	Ensure privacy governance, approve and oversee implementation of information security and privacy controls, review significant risks and corrective actions.
Data Protection Officer (DPO)	Advise on privacy obligations, review processing activities, monitor compliance, support data subject rights, maintain privacy registers, assist breach notification assessment and coordinate awareness.
Information Security Officer / Team	Implement and monitor security controls, support privacy incident response, perform access reviews, maintain technical safeguards and support audits.
Compliance / Legal / ISMS Team	Interpret legal/regulatory requirements, review contracts and DPAs, support DPIAs, monitor compliance and coordinate regulator-facing obligations.

Role	Responsibility
Data Owners	Define processing purpose, lawful basis, classification, access approvals, retention periods, sharing approvals and accuracy requirements.
System Owners	Ensure systems processing personal data implement approved security, access, logging, backup, retention and deletion controls.
HR / Training Team	Coordinate onboarding and annual privacy training, maintain attendance evidence and support disciplinary processes where required.
Procurement / Vendor Management	Ensure third-party privacy and security requirements are included in vendor due diligence, contracts and ongoing monitoring.
Employees / Contractors	Protect confidentiality, follow approved procedures, use data only for authorized purposes, complete training and report suspected incidents immediately.
Internal Audit	Perform periodic assessment of privacy controls, evidence, policy compliance and corrective action closure.

22 Review and Maintenance

This policy shall be reviewed at least annually or earlier where there are significant changes to applicable laws, ADHICS requirements, organizational structure, systems, processing activities, third-party arrangements, incidents or audit findings.

- The DPO, Information Security Officer and Compliance/Legal/ISMS Team shall support the review.
- Material changes shall be submitted for management approval before publication.
- Previous versions shall be retained according to document control and audit requirements.
- The policy owner shall ensure that obsolete versions are removed from active publication locations.

23 Mapping Frameworks to Standards

Framework / Requirement	Policy Coverage
ADHICS	Health information protection, confidentiality, privacy incident management, third-party security and information leakage controls.
ISO/IEC 27001:2022	Information security management controls including access control, incident management, supplier relationships, asset management, logging and compliance.
ISO/IEC 27701	Privacy information management, roles, privacy principles, data subject rights, controller/processor obligations and privacy risk management.
NESA UAE IAR	Information assurance, governance, access control, incident management and privacy/data protection requirements where applicable.
UAE PDPL	Lawful, fair and transparent processing; data subject rights; cross-border transfer control; security and breach management obligations where applicable.