RIVERSIDE MEDICAL CENTER, INC.

DR. PABLO O. TORRE MEMORIAL HOSPITAL

METRO PACIFIC HEALTH
THE HEART OF FILIPINO HEALTHCARE

DEPARTMENT: Office of the President		**POLICY NUMBER:** DPOTMH-APP-IT-P001 (01)	
TITLE/DESCRIPTION: **INFORMATION MANAGEMENT PLAN POLICY**			
EFFECTIVE DATE: July 30, 2025	REVISION DUE: July 29, 2028	**REPLACES NUMBER:** N/A	**NO. OF PAGES:** 1 of 11
APPLIES TO: All RMCI and Subsidiary Directors, Officers, Employees, and Medical Consultants ("Covered Personnel")		**POLICY TYPE:** Administrative	

PURPOSE:

To establish how the hospital governs, safeguards, and manages patient data (both clinical and administrative), and operational information. As a healthcare institution delivering patient-centric services, it is a must that a robust information management plan policy is in place to:

a. All hospital information management data are timely, relevant, and accurate.

b. Information or data must be compliant to all regulatory bodies (including but not limited to Philhealth, DOH, NPC, legal, ethical, and accreditation standards)

c. Information defined is used for continuity of quality care and improve patient outcomes

d. Adhere to the prime directive that all data contained in the infrastructure of the hospital is kept secure, confidential with appropriate access based on role and function, and maintain data integrity

e. Enable data-driven quality improvement initiatives and strategic planning

f. Adherence to the Data and Process Standards of MPH

DEFINITIONS:

Information Management Plan – documentation outlining how the hospital handles information throughout its lifecycle, ensuring security, confidentiality, compliance, and operational continuity.

Disaster Recovery – the hospital's processes to restore critical IT systems and data after a disruption to resume safe operations.

Recovery Time Objective – the maximum acceptable time allowed to restore a system after a disaster before it impacts hospital operations or patient care

Recovery Point Objective – the maximum amount of data loss (measured in time) the hospital can tolerate after a disaster, determining backup frequency

Hospital Information Management System – A secure, integrated digital platform the hospital uses to manage patient, clinical, and operational information such as EMR, billing, laboratory and imaging results, pharmacy, and reporting

Confidential Information – Any non-public hospital information that requires protection from unauthorized access or disclosure, including patient, staff, financial, and operational data.

Highly Confidential Information - The most sensitive hospital information requiring strict access control and enhanced protection, including medical records, credentials, security systems, and strategic documents.

DEPARTMENT: Office of the President		**POLICY NUMBER:** DPOTMH-APP-IT-P001 (01)	
TITLE/DESCRIPTION: **INFORMATION MANAGEMENT PLAN POLICY**			
EFFECTIVE DATE: July 30, 2025	REVISION DUE: July 29, 2028	**REPLACES NUMBER:** N/A	**NO. OF PAGES:** 2 of 11
APPLIES TO: All RMCI and Subsidiary Directors, Officers, Employees, and Medical Consultants ("Covered Personnel")		**POLICY TYPE:** Administrative	

RESPONSIBILITY:

a) All RMCI Employees, Clinicians (Consultants, Residents, PGI's, and other Physicians), Nurses, Allied Health Workers, and third-party Service Providers.

b) All Hospital Departments including Clinical, Administrative Support, and Ancillary Units

c) All users of information created, received, processed, stored, or transmitted through Information Systems used in RMCI (HIS/EMR, E-Claims, HRPIS, ERP, SyngoPlaza, Online Portals, and the likes)

POLICY:

The Riverside Medical Center, Inc. (RMCI) commits to effective, accurate, secure, and ethical management of all clinical, administrative, financial, and operational information by establishing a framework for its proper collection, storage, access, use, and disposal to support quality patient care, sound decision-making, regulatory compliance, and privacy protection. The Hospital upholds confidentiality, integrity, and availability of information through robust systems and procedures aligned with the Data Privacy Act of 2012, DOH standards, and Accreditation Canada International requirements, with all staff responsible for proper handling and timely reporting of any breaches or misuse. This policy is reviewed regularly to incorporate technological advancements, regulatory updates, and insights from evaluations and audits.

1. IN-SCOPE INFORMATION SYSTEMS

1.1. IQVIA Hospital Information System (HIS) w/ EMR

1.2. BizBox Hospital Information System & its components (Legacy System in use as part of data retention)

1.3. BizBox Beacon (E-Claims System)

1.4. RMCI Patient Portal

1.5. RMCI MD Portal for Consultants

1.6. RMCI Human Resource & Payroll Information System (HRPIS)

1.7. Online Leave Filing System

1.8. Picture Archiving and Communication System (PACS) – both online and on-premise

1.9. Laserfische Document Management System for scanning and archiving of physical charts

1.10. MAB-COSF Clinic Management System

2. CORE COMPONENTS

This section outlines the essential domains that form the foundation of an effective Hospital Information Management System. Each component supports clinical efficiency leading to improved patient outcomes, patient safety, legal compliance, and strategic planning.

2.1. Data Governance

Data governance provides a structured framework for managing information throughout its life cycle.

2.1.1. Ownership & Accountability:

All data and processes are assigned to specific data owners and or custodians

2.1.2. Policy Framework:

Includes policies on data classification, usage, and protection.

2.1.3. Standardization:

Use of standardized data definitions, coding systems (ICD10, RVS, LOINC, SNOMED CT), and naming conventions across departments.

2.1.4. Compliance:

Adherence to legal mandates such as the Data Privacy Act of 2012, DOH reporting requirements, Philhealth Circulars, BIR Requirements, and accreditation standards.

2.2. Data Collection & Capture

Effective data collection ensures accuracy and consistency from the point of entry.

2.2.1. Electronic and Paper Forms:

Use of validated, standardized forms and structured templates (e.g., clinical notes, admission forms).

2.2.2. Clinical Documentation:

Implement documentation standards (SOAP, SBAR) to support continuity of care.

2.2.3. Real-Time Data Entry:

Encouraged through EMRs and HIS for accuracy and timely access.

LIS ensures that all patient laboratory results are released to the HIS as soon as processing and validation is complete

Outpatients are informed in real-time the availability of their examination results in the Patient Portal via M360 SMS Service

2.2.4. Barcode/RFID Use:

For patient identification, specimen tracking, and inventory control.

2.3. **Data Storage & Retention**

Safe and organized storage protects records from loss, tampering, or unauthorized access.

2.3.1. Storage Systems:

2.3.1.1. Digital: On-premise automated backup stored in the data center of RMCI

2.3.1.2. Physical: Medical Records Storage with fireproof and water-resistant vault

2.3.2. Retention Periods:

2.3.2.1. Medical Records: Minimum 15 years for regular cases but no prescribed maximum period for Medico-legal related records (or as per DOH guidelines).

2.3.2.2. Financial Records: Minimum 10 years (as per BIR guidelines)

2.3.2.3. Employee Records: Minimum 10 years after separation.

2.3.3. Archiving:

Records past active use are archived securely and indexed for retrieval.

2.4. **Data Access & Sharing**

Controlled access protects privacy while supporting operational needs and care delivery.

2.4.1. Role-Based Access Control (RBAC):

Appropriate access is granted based on job role, function, and necessity. A general Access Matrix is followed in granting access.

2.4.2. Audit Trails:

Information Systems are equipped with electronic audit trails that is part and inherent in each system

2.4.3. Data Sharing:

2.4.3.1. Internal Sharing:

Information is shared through IT approved secure platforms such as Enterprise O365, VPNs, and Authenticated WAF access to online information systems

2.4.3.2. External Sharing:

RMCI shares patient and or employee data only when legitimate, lawful, and necessary for healthcare operations, reimbursements, or regulatory compliance using secure transmission methods and obtains patient/employee consent with inherent data sharing agreements. Authorized third parties include but not

DEPARTMENT: Office of the President		**POLICY NUMBER:** DPOTMH-APP-IT-P001 (01)	
TITLE/DESCRIPTION: **INFORMATION MANAGEMENT PLAN POLICY**			
EFFECTIVE DATE: July 30, 2025	REVISION DUE: July 29, 2028	**REPLACES NUMBER:** N/A	**NO. OF PAGES:** 5 of 11
APPLIES TO: All RMCI and Subsidiary Directors, Officers, Employees, and Medical Consultants ("Covered Personnel")		**POLICY TYPE:** Administrative	

limited to:

- Philhealth (Claims Processing)
- Health Maintenance Organizations
- Corporate Account Partners
- Department of Health (Mandatory Reporting)
- Financial Assistance Providers (PCSO, DSWD, LGU's, NGO's, and other partner charities)
- Accrediting Bodies
- External Auditor
- Enterprise Data Warehouse of MPH

2.4.4. Patient Access:

Patients have the right to access their own medical records as per hospital procedures.

Patients also have access to their records via the RMCI Patient Portal

2.5. **Privacy & Confidentiality**

Upholding ethical and legal responsibilities to protect patient and organizational data.

2.5.1. Policies:

Aligned with the Data Privacy Act of 2012 and hospital Code of Ethics.

2.5.2. Confidentiality Agreements:

Mandatory for all staff, trainees, and third-party contractors.

2.5.3. Consent Management:

Explicit patient consent is required for non-routine data use.

2.5.4. Data Breach Protocols:

Immediate reporting, investigation, and mitigation plans for any breach incident.

2.5.5. Physical Safeguards:

Locked cabinets, restricted access to record rooms, facial recognition door access system for hospital data center.

2.6. **Information Security**

Protects data from threats, unauthorized access, and disruptions.

2.6.1. Cybersecurity Measures:

2.6.1.1. Firewalls

2.6.1.2. Endpoint Protection

2.6.1.3. Data encryption (at rest and in transit)

2.6.1.4. Intrusion detection systems

2.6.1.5. 24/7 Managed Security Operations Center

2.6.1.6. 24/7 Managed Detection Response

2.6.2. User Authentication:

Implementation of Strong Password Policy

Two-factor Authentication for Privileged Users

Physical Security:

Closed Circuit Television Surveillance System

Facial Recognition Door Access Systems

2.6.3. Incident Response:

Security incident logging and rapid response team coordination

2.7. **Information Classification**

To properly manage access and use of information and or data, the hospital classifies data as follows

2.7.1. Public Information

Hospital announcements, approved marketing materials, publicly accessible reports, website, social media accounts, and community messaging boards

2.7.2. Internal Information

Departmental Communications, Internal Event and Meeting Schedules, Non-Sensitive operational douments

2.7.3. Confidential Information

- Patient Medical Records
- Clinical Documents (Examination Results and related forms)
- Billing information
- Employee Records
- Operational Reports
- Internal Policies

MASTER COPY

2.7.4. Highly Confidential Information

- Sensitive Patient Information (eg. HIV Status, Psychiatric Notes)
- Legal Documents and Internal Investigations
- Executive Decisions and Financial Audits
- Security and IT Infrastructure Details

2.8. **Business Continuity & Disaster Recovery**

Ensures information availability and operational restoration based on Recovery Time Objective.

2.8.1. Backup Procedures:

2.8.1.1. Daily automatic backups

2.8.1.2. Daily full database snapshots

2.8.2. Downtime Protocols:

2.8.2.1. Paper-based workflows during EMR/HIS outages

2.8.2.2. Manual tracking of admissions, orders, and medication

2.8.3. Redundancy:

2.8.3.1. Redundant UPS for Data Center

2.8.3.2. Active/Passive Firewall Configurations

2.8.3.3. Load Balancing Configuration between two (2) Internet Providers

2.8.4. Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) defined for key systems

2.8.5. Testing:

2.8.5.1. Annual disaster recovery drills including cyberattack simulations

2.8.5.2. Annual Vulnerability Assessment and Penetration Testing and Phishing Simulation

2.8.5.3. Evaluation and revision of protocols based on drill findings

3. ROLES AND RESPONSIBILITIES

ROLES	RESPONSIBILITIES
Executive Leadership (Mancom)	Provides governance, resources, and over-all strategic direction
Chief Information Officer (CIO)	Manages entire IT landscape including but not limited to: Process; Technology; People (part of Change Management), and Systems. Primary Responsibilities: a. Strategic Leadership b. Information Governance Oversight c. Information Security & Compliance d. Management of Information Systems e. Data Quality & Integrity Assurance f. Access Management Oversight g. IT Operations & Infrastructure Management
Data Protection Officer (DPO)	Ensures compliance with the Data Privacy Act Oversees breach management, PIAs, training, and privacy governance
Medical Records Officer	Manages safekeeping and archiving of patient physical records
Department Heads	Approve access levels for their staff Ensure accuracy and completeness of data (data quality) Enforce data confidentiality and privacy compliance in their units
RMCI Employees and Clinicians	Protect information according to Classification Use Information Systems Responsibly Report incidents or unauthorized access
Steering Committee	Conducts review of Information Management Plan policy and evaluates compliance with the Data Process Standards

DEPARTMENT: Office of the President		**POLICY NUMBER:** DPOTMH-APP-IT-P001 (01)	
TITLE/DESCRIPTION: **INFORMATION MANAGEMENT PLAN POLICY**			
EFFECTIVE DATE: July 30, 2025	REVISION DUE: July 29, 2028	**REPLACES NUMBER:** N/A	**NO. OF PAGES:** 9 of 11
APPLIES TO: All RMCI and Subsidiary Directors, Officers, Employees, and Medical Consultants ("Covered Personnel")		**POLICY TYPE:** Administrative	

4. TRAINING & CAPACITY BUILDING

4.1. Annual Data Privacy and Security Training.

4.2. Orientation for new hires on information handling.

4.3. Cybersecurity Threat Orientation

4.4. Specialized EMR/HIS user training by department.

5. CONTINUOUS IMPROVEMENT

5.1. Steering Committee conducts annual review of the plan.

5.2. Updates based on:

5.2.1. ACI accreditation feedback

5.2.2. Data Process Standards

5.2.3. Incident reports

5.2.4. New laws or technologies

5.2.5. Lessons from drills (e.g., cybersecurity, power outage)

DEPARTMENT: Office of the President		**POLICY NUMBER:** DPOTMH-APP-IT-P001 (01)	
TITLE/DESCRIPTION: **INFORMATION MANAGEMENT PLAN POLICY**			
EFFECTIVE DATE: July 30, 2025	REVISION DUE: July 29, 2028	**REPLACES NUMBER:** N/A	**NO. OF PAGES:** 10 of 11
APPLIES TO: All RMCI and Subsidiary Directors, Officers, Employees, and Medical Consultants ("Covered Personnel")		**POLICY TYPE:** Administrative	

PROCEDURES (SOP): N/A
WORK INSTRUCTION: N/A
WORK FLOW: N/A
FORMS: N/A
EQUIPMENT: N/A
REFERENCES: 1. Data Privacy Act of 2012 (RA 10173) 2. DOH Manual on Records Management 3. ISO 27701 – Privacy Information Management 4. Accreditation Canada – Information Management Standards

DEPARTMENT: Office of the President		**POLICY NUMBER:** DPOTMH-APP-IT-P001 (01)	
TITLE/DESCRIPTION: **INFORMATION MANAGEMENT PLAN POLICY**			
EFFECTIVE DATE: July 30, 2025	REVISION DUE: July 29, 2028	**REPLACES NUMBER:** N/A	**NO. OF PAGES:** 11 of 11
APPLIES TO: All RMCI and Subsidiary Directors, Officers, Employees, and Medical Consultants ("Covered Personnel")		**POLICY TYPE:** Administrative	

APPROVAL:				
	Name/Title	**Signature**	**Date**	**TQM Stamp**
Prepared by:	**CLAWY ANNE GARCIA-LUMIVES** Chief Information Officer		7/1/25	TQD
Reviewed by:	**WENDY MAE D. GOMEZ** Accreditation & Documentation Manager		7/3/25	
Approved by:	**RODEL J. LLAVE** Total Quality Division Head		7/7/25	
	SYLVESTER D. ALBA Sales and Marketing Division Head		7/9/25	
	JOASH B. TUMALA Logistics Division Head		7/11/25	
	HANNAH KHAY S. TREYES Chief Nursing Officer		7/15/25	
	JULIE ANNE CHRISTINE J. KO Chief Finance Officer		7/17/25	
	NOEL P. GARBO General Services Head		7/21/25	
	ROSARIO D. ABARING Ancillary Division Head		7/23/25	
	NANCY B. HIZON Human Resources Division Head		7/25/25	
	JOSE PEPITO B. MALAPITAN, MD Medical Director		7/29	
	MA. ANTONIA S. GENSOLI, MD VP/ Chief Medical Officer		7/30/25	
	SOCORRO VICTORIA L. DE LEON VP/ Chief Operating Officer		8/1/25	
Final Approved by:	**GENESIS GOLDI D. GOLINGAN** President and Chief Executive Officer		8/4/25	

MASTER COPY