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-DPO-P005-(01)	
TITLE/DESCRIPTION: **DATA BREACH RESPONSE POLICY**			
EFFECTIVE DATE: May 31, 2024	**REVISION DUE:** May 30, 2027	**REPLACES NUMBER:** N/A	**NO. OF PAGES:** 1 of 11
APPLIES TO: All RMCI Employees and third-party contacts that process the personal information of RMCI employees, clients, or patients		**POLICY TYPE:** Administrative	

PURPOSE:

This Data Breach Response Policy outlines the procedures and responsibilities for responding to data breaches within the Riverside Medical Center, Inc. and its third parties. This policy is designed to ensure a prompt, coordinated, and effective response to data breaches, including the identification of person or persons responsible for regular monitoring and evaluation of security incidents and the investigation of any suspected information security breach. RMCI aims to minimize the impact of breaches on individuals and uphold our commitment to protecting privacy and confidentiality.

DEFINITIONS:

Data Breach - as any unauthorized access, disclosure, or acquisition of personal information (PI) and sensitive personal information (SPI) that compromises the confidentiality, integrity, or availability of such data.

Security Incident - an event or occurrence that affects or tends to affect data protection, or may compromise the availability, integrity, and confidentiality of personal data.

Personal Information - any information that relates to a specific person (ex. employees, patients, clients, third-party vendors / partners). Some of the most obvious examples of personal information include someone's name, mailing address, email address, phone number.

Sensitive Personal Information – data that is subject to strict protection guidelines like, political beliefs, religious beliefs, genetic or biometric data, health information.

Mitigation measures - measures to minimize the impact of incidents while permanent solutions are developed.

Third Parties - any entity that RMCI does business with that involves the processing of personal information of the employees, clients, or patients. This includes suppliers, manufacturers, service providers, business partners, affiliates, brokers, distributors, resellers and agents, contractors, and temporary workers.

National Privacy Commission (NPC) - The National Privacy Commission is an independent body mandated to administer and implement the Data Privacy Act of 2012, and to monitor and ensure compliance of the country with international standards set for data protection.

RESPONSIBILITY:

Employee / Third-party, DPO, External Security Experts, Breach Response Team, IT and/or Concerned Department's Head

DEPARTMENT: Office of the President		**POLICY NUMBER:** DPOTMH-APP-DPO-P005-(01)	
TITLE/DESCRIPTION: **DATA BREACH RESPONSE POLICY**			
EFFECTIVE DATE: May 31, 2024	**REVISION DUE:** May 30, 2027	**REPLACES NUMBER:** N/A	**NO. OF PAGES:** 2 of 11
APPLIES TO: All RMCI Employees and third-party contacts that process the personal information of RMCI employees, clients, or patients		**POLICY TYPE:** Administrative	

POLICY:

1. **Discovery of Security Incidents**
   A security incident is any attempted or actual unauthorized access, use, disclosure, modification, or destruction of information. This includes interference with information technology operation and violation of company policies and procedures.

   The following are some of the most common types of security incidents among businesses and organizations:

- Theft – Incidents or events that resulted to the illegal transfer or storage of any personal data to unauthorized actors.
- Identity Fraud – Incidents or events that resulted to a successful attempt using someone's identity.
- Sabotage / Physical Damage – Incidents or events that resulted to an internal or external deliberate act of destruction or disruption of the organization's personal data processing activities.
- Malicious Code – Incidents or events that resulted to a malicious code causing damage to personal data processing system.
- Hacking – Incidents or events that resulted to intentionally accessing a computer system or personal data processing system without the authorization of the user or the owner.
- Misuse of Resources – Incidents or events that resulted to the deviation from the intended use of any element of a personal data processing system needed to perform required operations.
- Hardware Failure – Incidents or events that resulted to the termination of the ability of all or part of the physical components of a personal processing system to perform a required function.
- Software Failure – Incidents or events that resulted to the termination of the ability of all or part of the programs, procedures, rules, and associated documentation of a personal data processing system to perform a required function.
- Communication Failure – Incidents or events that resulted to the unexpected release of personal data through any communication means or platforms.
- Natural Disaster – Incidents or events that resulted to the abnormal intensity of a natural agent (flood, mudslide, earthquake, avalanche, drought) that caused availability issues.
- Design Error – Incidents or events that resulted to incorrect, incomplete, or poorly

DEPARTMENT: Office of the President		**POLICY NUMBER:** DPOTMH-APP-DPO-P005-(01)	
TITLE/DESCRIPTION: **DATA BREACH RESPONSE POLICY**			
EFFECTIVE DATE: May 31, 2024	**REVISION DUE:** May 30, 2027	**REPLACES NUMBER:** N/A	**NO. OF PAGES:** 3 of 11
APPLIES TO: All RMCI Employees and third-party contacts that process the personal information of RMCI employees, clients, or patients		**POLICY TYPE:** Administrative	

communicated design of a system or software to reduce the possibility of user making mistakes.

- User Error – Incidents or events that resulted to mistake of human action or inaction that produce an unintended result.
- Operations Error – Incidents or events that resulted due to improper execution of the organization's operational procedures.
- System Maintenance Error – Incidents or events that resulted to improper execution of software maintenance such as improving and boosting the software performance and correcting issues or bugs.
- Third Party / Service Provider – Incidents or events that exposed personal data of the organization caused by their official third-party partners or service providers.

There may also be other incidents or events that do not fall to the criteria mentioned above that may compromise the confidentiality, integrity, or availability of personal data. Such incidents should also be reported.

2. **Incident Reporting**
Communicating threats, risks, and hazards will help raise awareness of possible incidents and can ensure that preventive measures are in place.

Any employee or third-party who suspects or becomes aware of an incident that threatens data security, which may also be possible through complaints or feedback from clients or patients, must immediately report it to the designated Data Protection Officer (DPO) of RMCI through either of the following channels and with the details:

- Email:
Send to: privacy@rivermedcenter.net
Subject: Security Incident Report

- Details:
What kind of security incident are you reporting? Select all that apply from the incidents listed above.
Describe the incident.
When and how did the incident happen.

DEPARTMENT: Office of the President		**POLICY NUMBER:** DPOTMH-APP-DPO-P005-(01)	
TITLE/DESCRIPTION: **DATA BREACH RESPONSE POLICY**			
EFFECTIVE DATE: May 31, 2024	**REVISION DUE:** May 30, 2027	**REPLACES NUMBER:** N/A	**NO. OF PAGES:** 4 of 11
APPLIES TO: All RMCI Employees and third-party contacts that process the personal information of RMCI employees, clients, or patients		**POLICY TYPE:** Administrative	

Does this incident involve personal information?
How many individuals were affected?
Provide the names of the affected individuals if possible.

- Security incident Form
  Scan QR below:

3. **Initial Assessment and Evaluation**
   The initial assessment is conducted by the DPO and will coordinate with the Data Breach Response Team and Privacy Champion of the specific concerned department/s in gathering information to assess the scope and severity of the breach.

   The DPO will determine the kind of breach whether it is:
   - Availability breach. – from the loss accidental or unlawful destruction of personal data;
   - Integrity breach. – from the unauthorized alteration of personal data; and
   - Confidentiality breach. – from the unauthorized disclosure of or access to personal data.

   This will involve identifying the affected systems, the type and amount of data compromised, and potential risks to individuals. (Please see Annex A: Data Breach Response Team and Privacy Champions)

DEPARTMENT: Office of the President		**POLICY NUMBER:** DPOTMH-APP-DPO-P005-(01)	
TITLE/DESCRIPTION: **DATA BREACH RESPONSE POLICY**			
EFFECTIVE DATE: May 31, 2024	**REVISION DUE:** May 30, 2027	**REPLACES NUMBER:** N/A	**NO. OF PAGES:** 5 of 11
APPLIES TO: All RMCI Employees and third-party contacts that process the personal information of RMCI employees, clients, or patients		**POLICY TYPE:** Administrative	

4. **Containment and Mitigation**
   Immediate steps will be taken to contain the breach and mitigate its impact. This may include isolating affected systems, changing access credentials, or implementing temporary measures to prevent further unauthorized access. The IT Security and/or the department concerned will work to restore the integrity of the affected systems and data as quickly as possible.

5. **Notification**
   Once the breach has been contained and initial mitigation measures are in place, the DPO will assess the need for notification.

   The National Privacy Commission shall be notified within seventy-two (72) hours upon knowledge of or the reasonable belief by the personal information controller or personal information processor that a personal data breach has occurred.

   There can be no delay in the notification if the breach involves at least one hundred (100) data subjects, or the disclosure of sensitive personal information will harm or adversely affect the data subject. In either case, the Commission must be notified within the 72-hour period based on available information.

   The full report of the personal data breach must be submitted within five (5) days from notification, unless the personal information controller is granted additional time by the Commission to comply.

   Aside from notifying the NPC, the RMCI's Breach Response Team shall also notify the affected data subjects upon knowledge of, or when there is reasonable belief that a personal data breach has occurred. The obligation to notify remains with the personal information controller even if the processing of information is outsourced or subcontracted to a personal information processor.

   The failure to notify the NPC or the public is criminally liable for Concealment of Security Breaches Involving Sensitive Personal Information, which carries a corresponding penalty of imprisonment and fines.
   However, not all personal data breaches need to be notified to the National Privacy Commission

DEPARTMENT: Office of the President		**POLICY NUMBER:** DPOTMH-APP-DPO-P005-(01)	
TITLE/DESCRIPTION: **DATA BREACH RESPONSE POLICY**			
EFFECTIVE DATE: May 31, 2024	**REVISION DUE:** May 30, 2027	**REPLACES NUMBER:** N/A	**NO. OF PAGES:** 6 of 11
APPLIES TO: All RMCI Employees and third-party contacts that process the personal information of RMCI employees, clients, or patients		**POLICY TYPE:** Administrative	

and the affected data subjects. The DPO must be regularly updated on the guidelines provided by the NPC (https://privacy.gov.ph/) on Mandatory Notification.

6. **Investigation**
   A thorough investigation will be conducted to determine the cause of the breach, identify any vulnerabilities in security controls, and prevent future incidents.
   The investigation may involve forensic analysis, interviews with relevant personnel, and collaboration with external security experts if necessary.

7. **Remediation**
   Based on the findings of the investigation, appropriate remediation measures will be implemented to strengthen security controls and prevent similar breaches in the future.
   This may include enhancing policies and access controls, implementing encryption measures, or providing additional training to staff on data security best practices.

8. **Documentation and Reporting**
   All actions taken in response to the data breach, including containment efforts, notifications, and remediation activities, will be thoroughly documented.
   A comprehensive report will be prepared detailing the incident, the response process, and any lessons learned for future improvements.

9. **Communication**
   This policy will be communicated to all employees upon hire and made accessible through the RMCI's internal resources. Any updates or revisions to the policy will be promptly communicated to all relevant personnel.

This Data Breach Response Policy will be periodically reviewed and updated to ensure its effectiveness in addressing emerging threats and regulatory requirements.

Feedback from incident response exercises, audits, and regulatory changes will be incorporated into policy revisions.

DEPARTMENT: Office of the President		**POLICY NUMBER:** DPOTMH-APP-DPO-P005-(01)	
TITLE/DESCRIPTION: **DATA BREACH RESPONSE POLICY**			
EFFECTIVE DATE: May 31, 2024	**REVISION DUE:** May 30, 2027	**REPLACES NUMBER:** N/A	**NO. OF PAGES:** 7 of 11
APPLIES TO: All RMCI Employees and third-party contacts that process the personal information of RMCI employees, clients, or patients		**POLICY TYPE:** Administrative	

Annex A: Data Breach Response Team and Privacy Champions

I. DATA BREACH RESPONSE TEAM

Ancillary Division Officer	Ms. Rosario A. Abaring
Corporate Human Resource Officer	Ms. Nancy B. Hizon
Corporate Communication and Client Relations Manager	Mr. Geronimo Teofisto P. Estrella
Data Protection Officer	Ms. Nubbin E. Bito-on

II. DATA PRIVACY CHAMPIONS

Privacy champions are individuals within the organization who act as advocates for the organization's privacy program and serve as a direct liaison between their departments and the Privacy Office. A network of privacy champions across an organization helps to promote the privacy program and support engagement from a broad range of teams and stakeholders that would be otherwise challenging for the Privacy Office to reach and influence independently. Privacy champions may include those from different departments – particularly those functions interacting with personal data. Privacy champions can be made responsible for engaging with their colleagues, supporting with implementation of privacy initiatives or process changes, communicating ongoing training and awareness campaigns from the Privacy Office to their individual departments, and ensuring that policies and procedures are understood.

Ancillary Division	
Laboratory	Ms. Jessa Chris R. Negre / John L. Fernandez
Wellness	Ms. Eliza Oliva Esmeralda
Hemodialysis	Ms. Johairah Dirampa
PMFC	Ms. Ma. Teresa Anierdes
NICIS	Ms. Ma. Llana Linda Cardoñes 3/7/24
RTS	Ms. Shirley Malaga
DIS	Sir Bonifacio Sepico
Medical Service Division	
Clinical Chart Audit	Ms. Jean Suarez
Infection Control	Mr. Jhan Denver Dadula
Medical Records	Ms. Stella Marie Minette Año
Nursing Services	Ms. Hannah Treyes and Ms. Anne Montilla
Pharmacy	Ms. Sharlene Alintana
Engineering and General Services	
Engineering and Maintenance Department	Ms. Genesta May Ayomana-Pillo
Facilities Management	Ms. Lovelle Ochida
Security	Ms. Eva Sedayon
Logistics Division	Ms. Serjulyn Salazar
Total Quality Division	Sir Aldrian Abellar
Human Resource Division	Sir Peter Minguillo and Sir Roderick Pedral
Finance Division	Ms. Jemelyn Ferrer / Ms. Erma Grace Bandada
Sales and Marketing Division	Ms. Patricia Celia L. Coscolluela
IT	Sir Froilan Fuentes
Una Konsulta	Ms. Christine Genovia
MRCCC	Mr. Neil Ganchero

DEPARTMENT: Office of the President		**POLICY NUMBER:** DPOTMH-APP-DPO-P005-(01)	
TITLE/DESCRIPTION: **DATA BREACH RESPONSE POLICY**			
EFFECTIVE DATE: May 31, 2024	**REVISION DUE:** May 30, 2027	**REPLACES NUMBER:** N/A	**NO. OF PAGES:** 8 of 11
APPLIES TO: All RMCI Employees and third-party contacts that process the personal information of RMCI employees, clients, or patients		**POLICY TYPE:** Administrative	

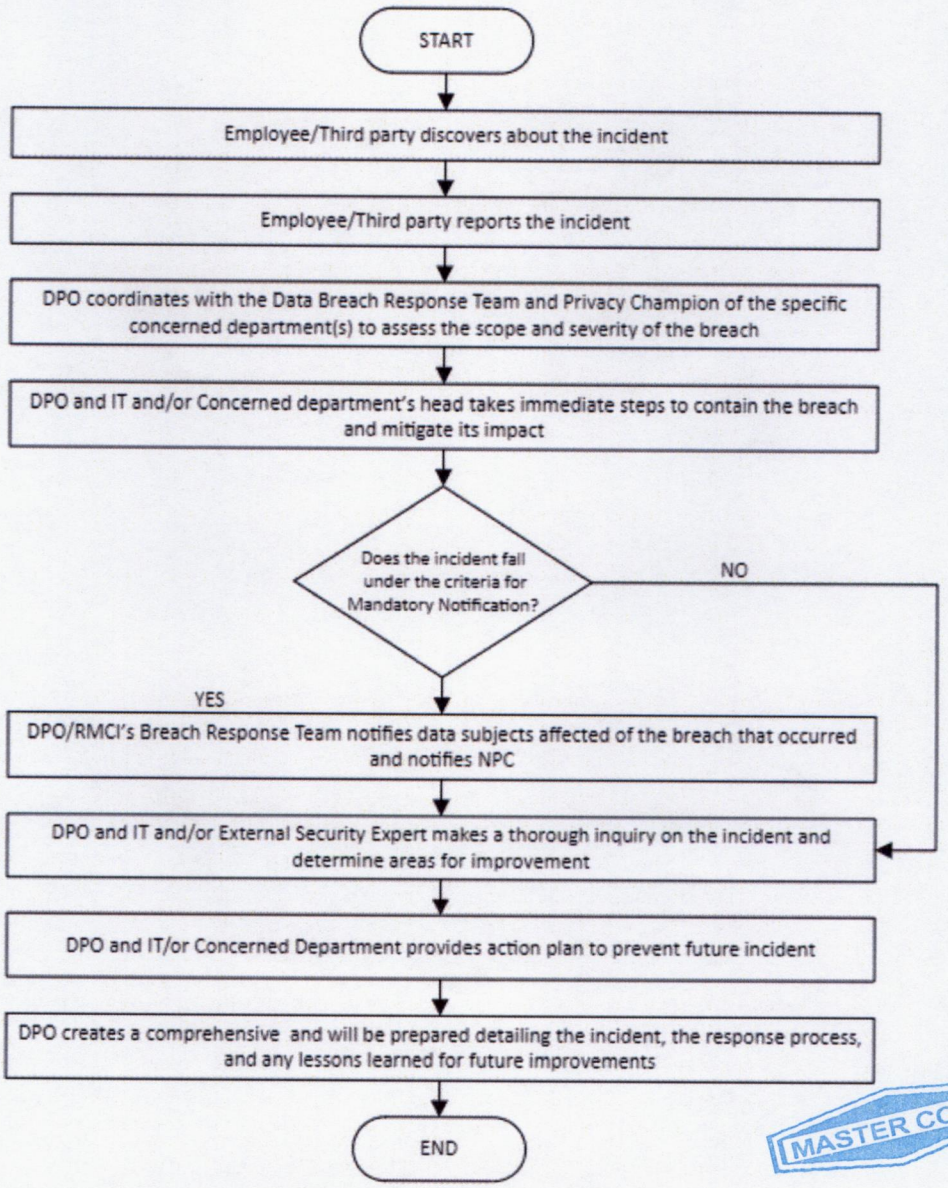
PROCEDURE (SOP): N/A

WORK INSTRUCTION:

KEY TASKS	PERSON RESPONSIBLE
1. Upon discovery or becoming aware of an event/ incident that may pose as a risk to data security, the individual reports the incident to the DPO.	Employee / Third-party
2. Assessing the scope and severity of the breach.	DPO, Breach Response Team, IT and/or Concerned department's head
3. Take immediate steps to contain the breach and mitigate its impact.	DPO and IT and/or Concerned department's head
4. Notify NPC and affected data subjects of the breach that occurred.	DPO and Data Breach Response Team
5. Make a thorough inquiry on the incident and determine areas for improvement.	DPO and/or external security experts
6. Provide action plans to prevent future incidents.	DPO and IT and/or Concerned department head
7. Create a comprehensive report.	DPO

DEPARTMENT: Office of the President		**POLICY NUMBER:** DPOTMH-APP-DPO-P005-(01)	
TITLE/DESCRIPTION: **DATA BREACH RESPONSE POLICY**			
EFFECTIVE DATE: May 31, 2024	**REVISION DUE:** May 30, 2027	**REPLACES NUMBER:** N/A	**NO. OF PAGES:** 9 of 11
APPLIES TO: All RMCI Employees and third-party contacts that process the personal information of RMCI employees, clients, or patients		**POLICY TYPE:** Administrative	

WORK FLOW:



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-DPO-P005-(01)	
TITLE/DESCRIPTION: **DATA BREACH RESPONSE POLICY**			
EFFECTIVE DATE: May 31, 2024	**REVISION DUE:** May 30, 2027	**REPLACES NUMBER:** N/A	**NO. OF PAGES:** 10 of 11
APPLIES TO: All RMCI Employees and third-party contacts that process the personal information of RMCI employees, clients, or patients		**POLICY TYPE:** Administrative	

FORMS: N/A

EQUIPMENT: N/A

REFERENCES:

1. https://privacy.gov.ph/pips-and-pics/breach-reporting/
2. https://privacy.gov.ph/exercising-breach-reporting-procedures/
3. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://privacy.gov.ph/wp-content/uploads/2017/08/03-Data-Breach-Prevention.pdf

MASTER COPY

RIVERSIDE MEDICAL CENTER, INC.

DR. PABLO O. TORRE MEMORIAL HOSPITAL

METRO PACIFIC HEALTH
THE HEART OF FILIPINO HEALTHCARE

DEPARTMENT: Data Privacy Office		**POLICY NUMBER:** DPOTMH-APP-DPO-P005-(01)	
TITLE/DESCRIPTION: **DATA BREACH RESPONSE POLICY**			
EFFECTIVE DATE: May 31, 2024	**REVISION DUE:** May 30, 2027	**REPLACES NUMBER:** N/A	**NO. OF PAGES:** 11 of 11
APPLIES TO: All RMCI Employees and third-party contacts that process the personal information of RMCI employees, clients, or patients		**POLICY TYPE:** Administrative	

APPROVAL:

	Name/Title	Signature	Date	TQM Stamp
Prepared by:	**NUBBIN BITO-ON** Data Protection Officer		4/29/24	TQD
Reviewed by:	**RODEL J. LLAVE** Total Quality Division Head		APR 24 2024	
Approved by:	**CLAWY ANNE LUMIVES** Chief Information Officer		May 21, 2024	
	MARIA LIZA C. PERAREN Nursing Director		MAY 24 2024	
	JULIE ANNE CHRISTINE J. KO Chief Finance Officer		5/28/2024	
	NOEL P. GARBO General Services Head		5/30/2024	
	ROSARIO D. ABARING Ancillary Division Head		05.30.2024	
	NANCY B. HIZON Human Resources Division Head		6/3/2024	
	MA. ANTONIA S. GENSOLI, MD VP/Chief Medical Officer		6-4-24	
	SOCORRO VICTORIA L. DE LEON VP/Chief Operating Officer		06/05/2024	
Final Approved by:	**GENESIS GOLDI D. GOLINGAN** President and Chief Executive Officer		06/10/24	

MASTER COPY