
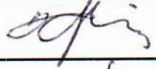

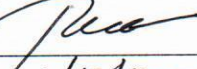
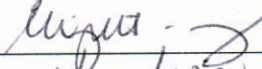
 A METRO PACIFIC HOSPITAL	Document Name:	Release Date:	Documentation No:
	Data Privacy Manual	Nov. 18, 2020	BPC-PO-19-009-00
	Department:	Version No.:	
	Business Process and Compliance	1.0.0	
Regulatory/ Standard Reference:		Page No.:	
RA 10173 (Data Privacy Act of 2012), Health Privacy Code of the Philippines (AO No. 2016-0002)		Page 1 of 130	
		Effectivity Date:	Expiry Date:
		Nov. 18, 2020	Nov 18, 2025

INFORMATION CLASSIFICATION LEVEL

- ☐ Level 0 – Public (or unclassified)
- ☐ Level 2 – Confidential
- ☒ Level 1 – Internal
- ☐ Level 3 – Restricted

	Prepared By	Reviewed By	Noted By	Recommending Approval by:	Approved By
Name	KARL MARXCUZ R. REYES	FREDERICK CHARLES G. RODRIGUEZ	OFELIA E. HERNANDO, RN, DEM	RANDY S. SAC	ELIZABETH G. DANTES, CPA, CMA
Role	Data Protection Officer	Head, Business Process and Compliance Department	Senior AVP, Hospital Operations	Chief Information Officer	President and CEO
Signature					
Date	11/18/20	11/18/20	18 Nov 2020	11/18/2020	11/19/2020


	Document Name:	Release Date:	Documentation No:
	Data Privacy Manual	Nov. 18, 2020	BPC-PO-19-009-00
	Department:	Version No.: 1.0.0	
	Business Process and Compliance	Page No.: Page 2 of 130	
Regulatory/ Standard Reference: RA 10173 (Data Privacy Act of 2012), Health Privacy Code of the Philippines (AO No. 2016-0002)		Effectivity Date: Nov. 18, 2020	Expiry Date: Nov 18, 2025

Table of Contents

I. Introduction..... 3

 Data Privacy Act of 2012 3

 National Privacy Commission 4

 Data Protection Officer 4

II. Definition of Terms..... 4

III. Scope and Limitations 9

IV. Processing of Personal Data..... 9

 Collection 10

 Use 14

 Disclosure 15

 Release of Personal Data..... 17

 Access 20

 Data Sharing 22

 Retention 23

 Disposal 23

 Data Quality..... 24

V. Security Measures..... 25

VI. Breach and Security Incidents..... 36

VII. Inquiries and Complaints..... 39

VIII. Effectivity..... 39

IX. References..... 40

X. Annexes..... 40

 DATA PRIVACY CONSENT FORM FOR EMPLOYEES 42

 CONFIDENTIALITY UNDERTAKING FORM 43

 DATA PRIVACY REQUEST FORM 45

 RECORDS DISPOSAL FORM 46

 PERSONAL DATA BREACH REPORT FORM 47

 WEBSITE DATA PRIVACY NOTICE 48

 DATA PRIVACY NOTICE 55

 DATA SHARING AGREEMENT..... 56

 DATA PRIVACY COMPLAINTS AND INQUIRIES PROCEDURE 61


 SECURITY INCIDENT RESPONSE POLICY AND PROCEDURE 65

 INFORMATION CLASSIFICATION POLICY 84

 RECORDS RETENTION AND DISPOSITION SCHEDULE 109

 DATA PROCESSING SYSTEMS INVENTORY 114

 DATA PRIVACY PENALTIES FOR VIOLATIONS..... 119

 A METRO PACIFIC HOSPITAL	Document Name:	Release Date:	Documentation No:
	Data Privacy Manual	Nov. 18, 2020	BPC-PO-19-009-00
	Department:	Version No.: 1.0.0	
	Business Process and Compliance	Page No.: Page 3 of 130	
Regulatory/ Standard Reference: RA 10173 (Data Privacy Act of 2012), Health Privacy Code of the Philippines (AO No. 2016-0002)		Effectivity Date: Nov. 18, 2020	Expiry Date: Nov 18, 2025

I. Introduction

Delos Santos Medical Center (“COMPANY”) is committed to provide the highest standard of healthcare service while ensuring the security and protection of the personal data it holds. In this regard, the company ensures that the rights of data subjects are respected and the culture of privacy is inculcated within the whole organization.

This Privacy Manual is hereby adopted in accordance with Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA), its implementing Rules and Regulations, and other relevant data protection laws, including issuances and advisories of the National Privacy Commission (NPC).

The organization adheres to the principles of transparency, legitimate purpose and proportionality and give the highest regard to the individual’s fundamental human right to privacy, and makes sure that all personal data collected from individuals, clients and patients are processed in adherence with the requirements of the Data Privacy Act of 2012.

This Manual aims to ensure that personal data in the organization’s data processing systems are secured and protected. It provides for the rules for processing of personal data and the obligations to be performed by the organization in relation to the processing of personal data. This Manual provides the organization’s data protection and security measures, and serves as a guide in exercising the data subject’s rights.

Data Privacy Act of 2012

Republic Act No. 10173 is an act protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, creating for this purpose a National Privacy Commission, and for other purposes.

The Data Privacy Act (DPA) is a strict privacy legislation “to protect the fundamental human right of privacy, of communication while ensuring free flow of information to promote innovation and growth.” (Ch 1, Sec 2.). Implicit in the DPA is the recognition that even as the law protects the right to privacy, it also articulates that free flow of information should be ensured.


The DPA assures that data protection is not an obstacle for people to obtain benefits from utilization of personal data. At the same time, it emphasizes that the use of personal data comes with a responsibility. The rights of data subjects should, at all times, be a paramount consideration.

The DPA applies to the processing of personal data by any natural and juridical person in the government or private sector. This includes processing of patient data by healthcare providers.

General obligations under the Data Privacy Act:

- 1. Adhere to Data Privacy Principles
- 2. Implement Security Measures
- 3. Uphold Rights of Data Subjects

For the official copy of the DPA, visit the NPC website: <https://privacy.gov.ph/data-privacy-act/>

	Document Name:	Release Date:	Documentation No:
	Data Privacy Manual	Nov. 18, 2020	BPC-PO-19-009-00
	Department:	Version No.: 1.0.0	
	Business Process and Compliance	Page No.: Page 4 of 130	
Regulatory/ Standard Reference: RA 10173 (Data Privacy Act of 2012), Health Privacy Code of the Philippines (AO No. 2016-0002)		Effectivity Date: Nov. 18, 2020	Expiry Date: Nov 18, 2025

National Privacy Commission

The National Privacy Commission (NPC) is the country’s privacy watchdog; an independent body mandated to administer and implement the DPA, and to monitor and ensure compliance of the country with international standards set for data protection.

The NPC protects individual personal information and upholds the right to privacy by regulating the processing of personal information.

The NPC is attached to the Department of Information and Communications Technology (DICT) and shall be headed by a Privacy Commissioner.

For the functions of the Commission, refer to [Chapter 1, Section 7 of the DPA](#), <https://privacy.gov.ph/data-privacy-act/#7>

Data Protection Officer

The person designated by DLSMC to have the primary function of monitoring compliance with the DPA, its Implementing Rules and Regulations and related issuances.

The Data Protection Officer (DPO) is the champion for privacy and data security within DLSMC, assisting management, healthcare professionals and employees cultivate best practices for the protection of personal data, and ensuring that health information technology providers providing services for the hospital likewise comply with the law.

The DPO must have expertise in DPA and a complete understanding of DLSMC’s IT infrastructure, technology and technical and organizational structure. The DPO manages the data protection and compliance internally while reporting non-compliance to proper authorities.

The following should be considered when designating a DPO:

- DPO should be knowledgeable on relevant privacy or data protection policies and practices
- DPO should understand the processing operations in the hospital, including laws and regulations that are relevant to the health sector
- DPO should be a full-time employee, or hired based on contract with term of at least 2 years
- There should be No Conflict of Interest if the DPO is performing other functions in the hospital
- The hospital should be ready to support the DPO in terms of providing resources and training to allow independent and effective performance of DPO functions


For full DPO guidelines, refer to the [NPC Advisory No. 2017-01 – Designation of Data Protection Officers](#), <https://privacy.gov.ph/data-privacy-act/#7>

II. Definition of Terms

Antivirus Software is a software utility that is designed to prevent, search for, detect and destroy known malicious files (e.g. viruses, worms, trojans, adware) from a computer.

Availability is the assurance that the systems responsible for delivering, storing and processing information are accessible when needed, by those who need them.

Consent refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of his or her personal, sensitive personal, or privileged information. Consent

 A METRO PACIFIC HOSPITAL	Document Name:	Release Date:	Documentation No:
	Data Privacy Manual	Nov. 18, 2020	BPC-PO-19-009-00
	Department:	Version No.: 1.0.0	
	Business Process and Compliance	Page No.: Page 5 of 130	
Regulatory/ Standard Reference: RA 10173 (Data Privacy Act of 2012), Health Privacy Code of the Philippines (AO No. 2016-0002)		Effectivity Date: Nov. 18, 2020	Expiry Date: Nov 18, 2025

shall be evidenced by written, electronic or recorded means. It may also be given on behalf of the data subject by an agent specifically authorized by the data subject to do so.

Confidentiality for the purposes of this Manual, confidentiality is a professional duty or a promise between a health practitioner and his or her patient that places restrictions on the disclosure or information provided by the patient as part of the care and treatment given by the practitioner. The duty of confidentiality is not absolute, and there are circumstances where a practitioner may lawfully disclose the patient’s information.

Conflict of Interest refers to a scenario wherein a DPO is charged with performing tasks, duties, and responsibilities that may be opposed to or could affect his performance as DPO. This includes, inter alia, holding a position within the organization that leads him to determine the purposes and the means of the processing of personal data.

Data refers to a representation of facts, concepts or instructions in a formalized manner suitable for communication, interpretation or processing by human beings or by automatic means.

Data Breach Response Team is a cross-disciplinary team created to bring in key personnel that will be needed to respond to a security incident or a personal data breach.

Data Processing Systems refers to the structure and procedure by which personal data is collected and further processed in an information and communications system or relevant filing system, including the purpose and intended output of the processing.

Data Sharing is the disclosure or transfer to a third party of personal data under the custody of a personal information controller or personal information processor. In the case of the latter, such disclosure or transfer must have been upon the instructions of the personal information controller concerned. The term excludes outsourcing, or the disclosure or transfer of personal data by a personal information controller to a personal information processor.

Data Sharing Agreement refers to a contract, joint issuance, or any similar document that contains the terms and conditions of a data sharing agreement between two or more parties: Provided, that only personal information controllers shall be made parties to a data sharing agreement.

Data Subject refers to an individual whose personal information is processed. (Ex. Patients, DLSMC employees).

Data Wiping sometimes referred to as **Data Clearing** or **Data Erasure** is a software-based method of overwriting the data that aims to completely destroy all electronic data residing on a hard disk drive.


De-identified Data is information or opinion about a person whose identity cannot be ascertained from the information or opinion.

Direct Marketing refers to communication by whatever means of any advertising or marketing material which is directed to particular individuals.

Disclosure is the act or process of revealing or uncovering a material fact or an item of information.

Disposal refers to any action that prevents the recovery of information from the storage medium on which it is recorded including, but not limited to, shredding, pulping, incineration, erasure, and destruction of the hardware or medium used to store and/or recovers the information.

Electronic Form or **Digital Record** or **Soft Copy** is information stored on electronic media, such as computer hard drives, copier, and printer hard drives, removable solid drives including memory, disks and USB flash drives, mobile phones and magnetic tapes.

	Document Name:	Release Date:	Documentation No:
	Data Privacy Manual	Nov. 18, 2020	BPC-PO-19-009-00
	Department:	Version No.: 1.0.0	
	Business Process and Compliance	Page No.: Page 6 of 130	
Regulatory/ Standard Reference: RA 10173 (Data Privacy Act of 2012), Health Privacy Code of the Philippines (AO No. 2016-0002)		Effectivity Date: Nov. 18, 2020	Expiry Date: Nov 18, 2025

Emergency is an unforeseen combination of circumstances that calls for immediate life-preserving or quality-of-life preserving actions (e.g., to preserve sight in one or both eyes, hearing in one or both ears, extremities at or above the ankle or wrist).

Encryption is the process of converting (encoding) information from a readable form (plain text) that can be read by everyone into an unreadable form (cipher text) that can only be read by the information owner and other authorized persons. It is a way of safeguarding data, documents, or information from threats such as malicious hackers, spies, criminals.

Filing System refers to any act of information relating to natural or juridical persons to the extent that, although the information is not processed by equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular person is readily accessible.

Firewall is a network security system designed to prevent unauthorized access to or from a private network. It acts as a barrier between a trusted system or network and outside connections, such as the internet.

Government Agency refers to a government branch, body, or entity, including national government agencies, bureaus, or offices, constitutional commissions, local government units, government-owned and controlled corporations, government financial institutions, government financial institutions, and state colleges and universities.

Hard Copy or **Paper-based Document** is the physical representation of data, such as paper printouts. This includes, among other things, notes, memos, messages, correspondence, transaction records and reports.

Health Care Provider is a health care institution devoted primarily to the management, treatment and care of patients, or a health care professional, who is any doctor of medicine, nurse, midwife, dentist, or other health care practitioner.

Health Information is any Personal information and sensitive personal information that relates to an individual’s past, present or future physical or mental health condition, including demographic data, diagnosis and management, medication history, health financing record, cost of services and any other information related to an individual’s total well-being. For purpose of A.O. 2016-0002, health information refers to personal health information which is individually identifiable information or de-identified health information.


Health Record is a documented account, whether in hard copy or electronic form, of a patient’s health, illness and treatment during each visit or stay at a health care institution.

Inpatient is a patient admitted to a health facility or hospital to receive healthcare services, including room, board and continuous nursing services in a unit area of the facility.

Information and Communications System refers to a system for generating, sending, receiving, storing or otherwise processing electronic data messages or electronic documents and includes the computer system or other similar device by or which data is recorded, transmitted or stored and any procedure related to the recording, transmission or storage of electronic data, electronic message, or electronic document.

Integrity is the trait that data or information have not been altered or destroyed in an unauthorized manner.

Lawful Heir or **Legal Assignee** is a person who is legally entitled to invoke the rights of the data subject, which he or she is an heir or assignee at any time after the death of the data subject or when the data subject is incapacitated or incapable of exercising the rights.

	Document Name:	Release Date:	Documentation No:
	Data Privacy Manual	Nov. 18, 2020	BPC-PO-19-009-00
	Department:	Version No.: 1.0.0	
	Business Process and Compliance	Page No.: Page 7 of 130	
Regulatory/ Standard Reference:		Effectivity Date:	Expiry Date:
RA 10173 (Data Privacy Act of 2012), Health Privacy Code of the Philippines (AO No. 2016-0002)		Nov. 18, 2020	Nov 18, 2025

Medical Privacy is the right to the protection of a person’s health information, which includes personal data, information about a patient’s condition as contained in medical records, and communications between healthcare provider and a patient.

Medical Record or Health Record is the primary repository of information concerning patient healthcare, which consists of a compilation of pertinent facts regarding a patient’s life history including past and present illnesses and treatments entered by a health professional contributing to the patient’s care.

Medical Staff refers to licensed physicians and other healthcare providers who are permitted by law and by a hospital to provide medical care within that hospital or facility.

Non-Disclosure Agreement (NDA) is a legal contract between at least two parties that outlines confidential material, knowledge, or information that the parties wish to share with one another for certain purposes.

Outpatient is a patient who receives medical care or healthcare services without being admitted and does not occupy a bed for any length of time. It may also refer to a patient who consults and receives healthcare services in the healthcare facility without being admitted.

Password is a confidential numeric and/or character string used in conjunction with a User ID to verify the identity of the individual attempting to gain access to a computer system.

Penetration Testing, colloquially known as **Pen-Testing**, is focused on simulating a real-life attack, testing defenses and mapping-out paths a real attacker could take to fulfill a real-world goal. This process confirms whether the vulnerability really exists and further proves that exploiting it can result in damage to the application or network.

Personal Data refers to all types of personal information (Personal information, Sensitive Personal Information).


Personal Data Breach refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed. A personal data breach may be in the nature of:

1. An availability breach resulting from loss, accidental or unlawful destruction of personal data;
2. Integrity breach resulting from alteration of personal data; and/or
3. A confidentiality breach resulting from the unauthorized disclosure of or access to personal data

Personal Information refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.

Personal Information Controller (PIC) refers to a person or organization who controls the collection, holding, processing or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use transfer or disclose personal information on his or her behalf.

Personal Information Processor (PIP) refers to any natural or juridical person qualified to act as such under this Act to whom a personal information controller may outsource the processing of personal data pertaining to a data subject.

	Document Name:	Release Date:	Documentation No:
	Data Privacy Manual	Nov. 18, 2020	BPC-PO-19-009-00
	Department:	Version No.: 1.0.0	
	Business Process and Compliance	Page No.: Page 8 of 130	
Regulatory/ Standard Reference: RA 10173 (Data Privacy Act of 2012), Health Privacy Code of the Philippines (AO No. 2016-0002)		Effectivity Date: Nov. 18, 2020	Expiry Date: Nov 18, 2025

Privacy Impact Assessment (PIA) helps a PIC and PIP navigate the process of understanding the personal data flows in the organization. It identifies and provides an assessment of various privacy risks, and proposes measures intended to address them.

Privacy Management Program (PMP) refers to a process intended to embed privacy and data protection in the strategic framework and daily operations of a personal information controller or personal information processor, maintained through organizational commitment and oversight of coordinated projects and activities.

Privacy Risk is the probability that the activity involving personal data will result in harm, or a loss of the rights and freedoms of an individual. Controls may be applied in order to reduce severity, likelihood, and magnitude of the privacy risk.

Privileged Information refers to any and all forms of data which under the Rules of Court and other pertinent laws constitute privileged communication.

Processing refers to any operation or set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data. (Ex. Storing Medical Records, Release of Medical Abstracts, responding to subpoena).

Profiling refers to any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

Research is a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

Security a tangible set of physical and logical mechanisms which can be used to protect information held in hard and soft copy, digital format, within computer systems, via telecommunications infrastructure, etc.

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


Security Incident Management Policy refers to policies and procedures implemented by a PIC or PIP to govern the actions to be taken in case of security incident or personal data breach.

Sensitive Personal Information refers to the following personal information:

- Race
 - Ethnic origin
 - Marital status
 - Education
 - Genetic or sexual life
 - Previous or Current Health Records
 - Issued by Government Agencies
- Age
 - Color
 - Health
 - Social Security Number
 - Licenses
 - Tax Returns
 - Religious, philosophical or political affiliations

Third Party refers to any person, entity or institution other than the patient, healthcare provider or health facility, or any other duly authorized personal information processor or person desiring to have access to patient’s health information (i.e. HMOs, researchers, among others).

Threat refers to a potential cause of an unwanted incident, which may result in harm or danger to a data subject, system, or organization.

 A METRO PACIFIC HOSPITAL	Document Name:	Release Date:	Documentation No:
	Data Privacy Manual	Nov. 18, 2020	BPC-PO-19-009-00
	Department:	Version No.: 1.0.0	
	Business Process and Compliance	Page No.: Page 9 of 130	
Regulatory/ Standard Reference: RA 10173 (Data Privacy Act of 2012), Health Privacy Code of the Philippines (AO No. 2016-0002)		Effectivity Date: Nov. 18, 2020	Expiry Date: Nov 18, 2025

Unsecured Work Area an open workstation or area that cannot be locked to prohibit entry.

User ID is a unique identifier given to an individual allowing that individual access to a computer system. A User ID is usually accompanied by a password.

Vulnerability refers to a weakness of a data processing system that makes it susceptible to threats and other attacks.

Vulnerability Assessment is the process of finding and measuring the severity of vulnerabilities in a system. It yields lists of vulnerabilities, often prioritized by severity and/or business criticality.

Workstation is a computer used for running software applications, storing, and transmitting data. In networking, workstation refers to any computer (desktop or laptop) connected to a local area network.

III. Scope and Limitations

This Manual shall apply to all physicians (active and visiting consultants, and residents), DLSMC employees including health professionals (nurses and ancillary personnel), including students or interns in training, practicing their profession, working, or fulfilling academic and clinical requirements within DLSMC, whether temporary or permanent.

It shall also apply to all personnel of this organization, regardless of the type of employment or contractual arrangement, including business partners, such as Janitorial services, Security services, Spiritual Care services, HMO and Corporate partners and other third parties who interact with personal data held by DLSMC and the information systems used to store and process it.

This Manual is limited to personal data processed by DLSMC including the tools and equipment involved in personal data processing.


This privacy manual shall be read in conjunction with all other existing policies of Delos Santos Medical Center such as but not limited to the relevant Human Resource Policies and Procedures, Business Process and Compliance Policies and Information Security Policies on the collection, use, disclosure, sharing, retention and disposal of personal data.

IV. Processing of Personal Data

The processing of personal information shall be allowed, in accordance with the requirements of the Data Privacy Act of 2012 and other laws allowing disclosure of information to the public and in adherence to the principles of transparency, legitimate purpose and proportionality.

Transparency. The data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguard involved, the identity of personal information controller, his or her rights as a data subject, and how these can be exercised. Any information and communication relating to processing of personal data should be easy to access and understand, using clear and plain language.

Legitimate Purpose. The processing of information shall be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy. Processing of personal data should have the individual’s consent, or must be authorized or allowed by the Constitution or by law.

	Document Name:	Release Date:	Documentation No:
	Data Privacy Manual	Nov. 18, 2020	BPC-PO-19-009-00
	Department:	Version No.: 1.0.0	
	Business Process and Compliance	Page No.: Page 10 of 130	
Regulatory/ Standard Reference: RA 10173 (Data Privacy Act of 2012), Health Privacy Code of the Philippines (AO No. 2016-0002)		Effectivity Date: Nov. 18, 2020	Expiry Date: Nov 18, 2025

Proportionality. The processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.

The processing of personal data shall adhere to the following general principles in the collection, use, access, disclosure, sharing, release, retention and destruction.

Criteria for Lawful Processing

Personal Information:


- 1. Consent is given by data subject;
- 2. Performance of contract or non-commercial activities;
- 3. Necessary for compliance with legal obligation;
- 4. Necessary to protect interest of data subject;
- 5. Necessary to respond to national emergency;
- 6. Performance of mandate of a public authority;
- 7.Necessary to pursue legitimate interest of personal information controller.

Sensitive Personal Information and Privileged Information:

- 1. Consent is given by data subject;
- 2. The processing of the same is provided for by existing laws and regulation
- 3. The processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing;
- 4. The processing is necessary to achieve the lawful and non-commercial objectives of public organizations and their associations;
- 5. The processing is necessary for purposes of medical treatment;
- 6. The processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings.

Collection

- 1. Adhering to the principle of Proportionality, Personal Data to be collected should be adequate, relevant, suitable, necessary and not excessive to the legitimate purpose.
 - 1.1. Authorized personnel to collect personal data from data subjects:
 - 1.1.1. Medical Staff and Admission Staff are allowed to collect patient personal data for purposes relating to health care and treatment.
 - 1.1.2. Human Resources Staff are allowed to collect personal data of DLSMC employees or applicants for purposes of employee management and personnel recruitment.
 - 1.1.3. Medical Affairs Staff are allowed to collect personal data of applicants for Residency and Internship programs of DLSMC.
 - 1.1.4. Customer Care Staff are allowed to collect personal data of persons who has inquiries or complaints submitted using DLSMC’s website, phone calls, emails or post mails.
 - 1.1.5. Marketing Staff are allowed to collect personal data of persons who attended or participated in their promotional events.

	Document Name:	Release Date:	Documentation No:
	Data Privacy Manual	Nov. 18, 2020	BPC-PO-19-009-00
	Department:	Version No.: 1.0.0	
	Business Process and Compliance	Page No.: Page 11 of 130	
Regulatory/ Standard Reference: RA 10173 (Data Privacy Act of 2012), Health Privacy Code of the Philippines (AO No. 2016-0002)	Effectivity Date:		Expiry Date:
	Nov. 18, 2020		Nov 18, 2025

1.1.6. Security Officers and Personnel are allowed to collect personal data from all individual within DLSMC premises by monitoring surveillance equipment and by taking logs in the ingress and egress of the company.

1.2. Information on collection and processing of Personal Data of the Data Subject shall be relayed to the Data Subject through a Privacy Notice. The company’s authorized personnel shall inform the data subject of the purpose/s for the collection of personal data, extent of processing and the rights of data subjects.

1.3. Consent - should be freely given and specific. It must be an informed indication of will whereby a data subject agrees to the collection and processing of personal data.

1.2.1. Obtaining Consent from data subjects should be done prior to the processing of personal data.

1.3.1.1. Consent is required prior to the collection, or as soon as practicable and reasonable, of personal data from different data subject categories.

1.3.1.1.1. In-patients - for every admission to the hospital.

1.3.1.1.2. Out-patients - for every availment of DLSMC’s health services where personal data is processed by DLSMC.

1.3.1.1.3. Applicants, On the Job Trainees, Office Interns, Medical Residents, Medical Interns - whenever they apply for work in DLSMC.

1.3.1.1.4. Employees, Office Consultants – during on-boarding activities when they start to work for DLSMC.

1.3.1.2. DLSMC Staff authorized to collect personal data should ensure that the data subject understands the content of the consent form and the processing activities involved therein.

1.3.1.3. Consent must be obtained directly from the data subject who has the capacity to perform as such.


1.3.1.3.1. For data subjects who is a minor (below 18 years old) or who is incapacitated or incapable of giving consent, the lawful heirs, legal assignee or a guardian may give the consent on behalf of the minor or the incapacitated person.

1.3.1.3.2. For representatives or a person with legal authority, legal documents – such as birth certificate, marriage certificate and similar documents – must be presented to establish the relationship between the data subject and the authorized person.

1.3.1.4. Consent shall be given by a patient of legal age and sound mind, or in cases where a data subject is incapacitated to give consent, any of the following provided here under can give consent:

- (a) Those related within the third degree of consanguinity or affinity in accordance with the order of preference under applicable laws;
- (b) Common Law wife;
- (c) Social worker;

1.2.1.4.1 if a patient has a duly executed advance directive or power of attorney for healthcare, the same shall be given effect.

	Document Name:	Release Date:	Documentation No:
	Data Privacy Manual	Nov. 18, 2020	BPC-PO-19-009-00
	Department:	Version No.: 1.0.0	
	Business Process and Compliance	Page No.: Page 12 of 130	
Regulatory/ Standard Reference: RA 10173 (Data Privacy Act of 2012), Health Privacy Code of the Philippines (AO No. 2016-0002)		Effectivity Date: Nov. 18, 2020	Expiry Date: Nov 18, 2025

1.3.1.5. The consent should be evidenced by written, electronic or recorded means.

1.3.1.6. Adhering to the principle of Transparency, consent should not be Implied, assumed, coerced and convinced.

1.3.2. Composition of Consent

1.3.2.1. Should indicate the nature, specific purpose and extent of processing personal data. This includes sharing information with affiliates or even the mother company or third parties in proper cases.

1.3.2.2. Risks and safeguards of personal data processing should be considered in the consent form.

1.3.2.3. Validity of consent should cover the data processing lifecycle of collection, use, distribution or sharing, retention, disclosure and disposal.

1.3.2.4. Should be written in plain and clear language.

- 1.3.2.5. Should contain at least:
- a. Full name of the data subject
 - b. Date of written consent
 - c. Name of person being authorized and their relationship to the data subject if the data subject is not capable of giving consent

1.3.3. Consent is not required on the following conditions:

1.3.3.1. For Personal Information

1.3.3.1.1. Publicly available personal data that will be processed for research purpose, intended for a public benefit, subject to the requirements of applicable laws, regulations, or ethical standards.

1.3.3.1.2. To fulfill contractual obligations with data subject (ex. Processing by billing section).


1.3.3.1.3. The processing is necessary to protect vitally important interests of the data subject, including his or her life and health (ex. Contact tracing).

1.3.3.2. For Sensitive Personal Information


1.3.3.2.1. The processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing. (ex. Public health emergency, finding next of kin of unconscious patient).

1.3.3.2.2. Processing is provided for by existing laws and regulations, where personal data protection is guaranteed and consent is not required. (ex. HIV/AIDS contact tracing and all other related health intelligence activities pursued by DOH).

1.3.3.2.3. Processing for purpose of medical treatment, carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal data is ensured (ex. Creating a Health Record).

	Document Name:	Release Date:	Documentation No:
	Data Privacy Manual	Nov. 18, 2020	BPC-PO-19-009-00
	Department:	Version No.: 1.0.0	
	Business Process and Compliance	Page No.: Page 13 of 130	
Regulatory/ Standard Reference: RA 10173 (Data Privacy Act of 2012), Health Privacy Code of the Philippines (AO No. 2016-0002)		Effectivity Date: Nov. 18, 2020	Expiry Date: Nov 18, 2025


- 1.3.3.2.4. Processing is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise, or defense of legal claims, or when provided to government or public authority pursuant to a constitutional or statutory mandate (ex. Defending against a case filed against hospital)
- 1.3.3.3. Other Exemptions. Consent shall not be required for the processing of personal data in the PHIE under the following conditions:
- (a) For purpose of medical treatment, carried out by a medical practitioner or a medical treatment institution;
 - (b) When necessary to protect the life and health of the patient or another person, and the patient is not legally or physically able to express his or her consent prior to the processing;
 - (c) When processing is required by existing law and regulation, such as, but not limited to:
 - (1) Act 3573: law of reporting of communicable diseases;
 - (2) Administrative Order No. 2008-0009: Adopting the 2008 revised list of notifiable diseases, syndromes, health-related events and conditions.
- 1.3.3.3.1. The processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing. (ex. Public health emergency, finding next of kin of unconscious patient).
- 1.3.3.3.2. Processing is provided for by existing laws and regulations, where personal data protection is guaranteed and consent is not required. (ex. HIV/AIDS contact tracing and all other related health intelligence activities pursued by DOH).
- 1.3.3.3.3. Processing for purpose of medical treatment, carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal data is ensured (ex. Creating a Health Record).
- 1.3.3.3.4. Processing is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise, or defense of legal claims, or when provided to government or public authority pursuant to a constitutional or statutory mandate (ex. Defending against a case filed against hospital).
- 1.2.4. Withdrawal/Objection of Consent
- 1.3.4.1. Data subjects with capacity to withdraw or to object consent may do so at any time.
- 1.3.4.1.1. The data subject should provide DLSMC with written notification of the withdrawal or objection of their consent by accomplishing the data subject request form annexed in this privacy manual.
 - 1.3.4.1.2. Once withdrawn, data subject request form evidencing withdrawal shall be attached to the records of the data subject followed by applying the existing ***Records Retention and Disposition Schedule***.
- 1.3.4.2. Withdrawal of personal data processing must be clear, voluntary and unambiguous.

	Document Name:	Release Date:	Documentation No:
	Data Privacy Manual	Nov. 18, 2020	BPC-PO-19-009-00
	Department:	Version No.: 1.0.0	
	Business Process and Compliance	Page No.: Page 14 of 130	
Regulatory/ Standard Reference: RA 10173 (Data Privacy Act of 2012), Health Privacy Code of the Philippines (AO No. 2016-0002)		Effectivity Date: Nov. 18, 2020	Expiry Date: Nov 18, 2025

1.3.4.3. An authorized representative or a person with legal authority who consented on the data subject’s behalf may also withdraw the consent.

Use

- 2. Use of Personal Data collected from data subjects must be according to the declared, specified and legitimate purpose.
 - 2.1. It is the policy of DLSMC to ensure that only authorized personnel have access to its patient’s or employee’s personal data.
 - 2.2. The purpose of the use of the data subject’s personal data must be included in the consent form. Furthermore, the use of the personal data should be in line with which the data subject has consented.
 - 2.3. DLSMC may use personal data collected for the primary purpose for which it was collected. The primary purpose will generally be the dominant purpose for which the information was collected.
 - 2.4. DLSMC may use the personal data it has collected about a data subject if it is directly related purpose to the primary purpose and the data subject would reasonably expect DLSMC to use the information for this purpose.
 - 2.4.1. For the purpose of obtaining payment, processing, monitoring, verifying or reimbursing claims for payment, or preventing any unauthorized receipt of related services or benefits (which includes debt collection for health care or related goods or services).
 - 2.4.2. For planning risk management or in order to improve or maintain the quality of healthcare services.
 - 2.5. Personal data shall not be used for purposes other than those for which it was collected, except with the consent of the data subject or as required by law.
 - 2.6. Should personal data be used for the purpose of research:
 - 2.6.1. Data collected from parties other than the data subject for purpose of research shall be allowed when personal data is publicly available.
 - 2.6.2. If data is not publicly available, the data subject has consented that his or her personal data will be used for research.
 - 2.6.3. Adequate safeguards should be in place and no decision directly affecting the data subject shall be made on the basis of the data collected or processed.
 - 2.6.4. The personal data used in the research activity should be de-identified.
 - 2.6.5. The rights of the data subject shall be upheld without compromising research integrity.
 - 2.7. Should personal data be used for the purpose of training:
 - 2.7.1. The anonymity of the data subject should be maintained or the personal data be de-identified during case presentations, demonstrations, research activities and at seminars and conferences.
 - 2.7.2. Use of photos, slides and other visual aids which allow identification of individuals should not occur unless the consent of the data subject has been obtained.

	Document Name:	Release Date:	Documentation No:
	Data Privacy Manual	Nov. 18, 2020	BPC-PO-19-009-00
	Department:	Version No.: 1.0.0	
	Business Process and Compliance	Page No.: Page 15 of 130	
Regulatory/ Standard Reference: RA 10173 (Data Privacy Act of 2012), Health Privacy Code of the Philippines (AO No. 2016-0002)		Effectivity Date: Nov. 18, 2020	Expiry Date: Nov 18, 2025

2.8. Personal data used for DLSMC’s Chaplaincy services:

- 2.8.1. Consent forms should indicate that patient information may be provided to accredited priests, chaplains or any Spiritual Care workers of DLSMC.
- 2.8.2. Further information about the patient’s health care treatment may also be disclosed to the accredited priest, chaplain or Spiritual Care worker (including volunteers) involved in the patient’s care if this is considered by the medical treating team to be relevant and appropriate.
- 2.8.3. The patient may indicate at any time if they do not wish to receive Spiritual Care services or if they do not want their information to be made available to accredited priests, chaplains and pastoral care workers (including volunteers).

2.9. Personal data used for Marketing:

- 2.9.1. Personal data may be used to contact data subjects with newsletters, updates, information campaigns, marketing or promotional materials and other information that may be related to the services that DLSMC provide, and to further improve the quality of services.

2.10. Whenever DLSMC Staff is using personal data, the policies for *Clean Desk and Clear Screen* must be applied.

- 2.10.1. Data subject can withdraw or object the use or processing of his or her personal data. If, during a non-medical processing of personal data, the data subject indicates he or she wants the processing of his or her personal data to stop, the staff should stop the processing and then explain the consequences of not proceeding further, without implying coercion.


2.11. The IT department, with the supervision of the DPO shall be in-charge to monitor and limit access to electronic media / devices, computer systems and any other IT-related facilities used in the company.

Disclosure

- 3.1 Disclosure of Personal Data shall be undertaken in a manner that ensures appropriate privacy and security safeguards. All employees and personnel of the company shall maintain the confidentiality and secrecy of all personal data that come to their knowledge and possession, even after resignation, termination of contract, or other contractual relations. Personal data under the custody of the company shall be disclosed only pursuant to a lawful purpose, and to authorized recipients of such data.

3.2 Data sharing shall be allowed:

- i. When it is expressly authorized by law;
- ii. If the data subject consents to data sharing;
- iii. When the personal data is publicly available, or has the consent of the data subject for purpose of research;
- iv. When covered by a “Data Sharing Agreement”.

	Document Name:	Release Date:	Documentation No:
	Data Privacy Manual	Nov. 18, 2020	BPC-PO-19-009-00
	Department:	Version No.: 1.0.0	
	Business Process and Compliance	Page No.: Page 16 of 130	
Regulatory/ Standard Reference: RA 10173 (Data Privacy Act of 2012), Health Privacy Code of the Philippines (AO No. 2016-0002)		Effectivity Date: Nov. 18, 2020	Expiry Date: Nov 18, 2025


3.3 The company shall maintain a Data Sharing Agreement (DSA) will all its Third Party service providers, partners, subsidiaries, and clients where personal data are being shared. The DPO, with the assistance of the Business Process Department shall monitor and see to it that DSAs are properly in place.

3.4 DLSMC may disclose personal data to other third parties, including regulatory authorities, government agencies, as well as parties with whom the data subject voluntarily transact.

- 3.4.1 For the performance of legal obligation, DLSMC may disclose personal data to government authorities (ex. provision of documentary and/or testimonial evidence in court proceedings)
- 3.4.2 Employee Data shall not be disclosed by DLSMC through its Human Resources Department without authorization from the employee itself.
- 3.4.3 Third-parties or any entity conducting background verification or background check shall only be entertained by the Human Resources Department provided a consent was secured from the employee.
- 3.4.4 There shall be no instance that the Human Resources Department will be held accountable for compromise of personal data consented by the employee. The Human Resources Department shall only be responsible for verifying the correctness of the personal data disclosed by the employee itself.
- 3.4.5 Employees shall expressly indicate their consent in the disclosure of their personal data to any entity they voluntarily transact by filling up the Data Privacy Request Form and checking the “access to personal data” query and indicate the purpose of such access. A Waiver Form shall also be accomplished by the employee thereby releasing DLSMC from any liability arising from such disclosure caused by the employee. The Data Privacy Request Form shall then be submitted to the Human Resources Department. The forms indicated above shall constitute notice and authority granted by the employee whose data is requested to be disclosed.
- 3.4.6 DLSMC employees may not disclose personal data to legal authorities such as police officers or lawyers without the consent of the data subject (ex. Patient, his or her legal assignee, or employee) unless there is a valid search warrant or subpoena issued. The subpoena should specify the type of information requested.

2.12. For medical diagnosis and treatment, DLSMC will disclose personal data to physicians and medical staff, affiliates, related entities and authorized partners, including third parties, as part of its regular business operations.

- 2.12.1. For Special Laboratory Tests, in-patient specimen may be tested by third party affiliates. This procedure should adhere to the Data Sharing Agreement conditions stated in this manual.
- 2.12.2. Other persons involved or interested in the data subject’s healthcare, such as family members, loved ones or any other person involved in the data subject’s healthcare.

 A METRO PACIFIC HOSPITAL	Document Name:	Release Date:	Documentation No:
	Data Privacy Manual	Nov. 18, 2020	BPC-PO-19-009-00
	Department:	Version No.: 1.0.0	
	Business Process and Compliance	Page No.: Page 17 of 130	
Regulatory/ Standard Reference: RA 10173 (Data Privacy Act of 2012), Health Privacy Code of the Philippines (AO No. 2016-0002)		Effectivity Date: Nov. 18, 2020	Expiry Date: Nov 18, 2025

2.13. For benefits, payments and claims, DLSMC may disclose the nature and type of treatment and other related information that will be required for settlement.

2.13.1. It is normally sufficient for DLSMC to provide a medical report for claims to be processed. If further information is requested, only relevant sections of the patient’s health record may be provided. (ex. Disclosure of medical report to HMO or Corporate partners).

2.13.2. Patient consent is required for disclosure of additional health records.

2.14. Disclosure of Personal Data should be done by a DLSMC staff who is authorized to do so.

2.14.1. For patient data involving the Medical Certificate, Operative Records, Histopathology Results, Abstract and Discharged Summary, Certificate of Confinement, Medico-Legal Certificate and Laboratory Examination Results sanctioned by De Los Santos Medical Center shall only be released and/or disclosed by and with the Medical Records through its Centralized Request and Releasing Section and determined releasing section of the Ancillary Units of DLSMC.

2.14.2. Other data in addition to the abovementioned patient data which requires dry seal of DLSMC must be done only by the Medical Records.

2.14.3. For employee data, the Human Resources Department in accordance with the existing policies regarding disclosure shall only be allowed to disclose employee personal data upon satisfaction of the requisites stated under this manual.

2.15. Implement the *Clean Desk and Clear Screen* policies:

2.15.1. Do not take any personal data (including patient data) in electronic form outside office without proper security measures such as encryption or setting up a password or enclosing the paper-based personal data in a sealed envelope.

2.15.2. Do not disclose patient information in public or over the phone (having a conversation with fellow DLSMC medical staff).

2.15.3. Do not discuss patient health information in public areas of the hospital, including the lobby of the hospital, elevator or cafeteria.

2.15.4. DLSMC employees should ensure that unauthorized persons are unable to view personal data whether held on paper documents or information displayed on workstation monitors.


2.15.5. Other prohibitions can be seen in the *DLSMC’s Clean Desk and Clear Screen Policies*.

2.15.6. A Non-Disclosure Agreement is required whenever an employee, medical staff, interns, on-the-job trainees, third party or external service providers have access to and use of any personal data while discharging their function.

2.15.7. All employees and personnel of the company shall maintain the confidentiality and secrecy of all personal data that come to their knowledge and possession, even after resignation, termination of contract, or other contractual relations.

Release of Personal Data

4. Releasing of Personal Data shall be undertaken in a manner that ensures appropriate security safeguards.

	Document Name:	Release Date:	Documentation No:
	Data Privacy Manual	Nov. 18, 2020	BPC-PO-19-009-00
	Department:	Version No.: 1.0.0	
	Business Process and Compliance	Page No.: Page 18 of 130	
Regulatory/ Standard Reference: RA 10173 (Data Privacy Act of 2012), Health Privacy Code of the Philippines (AO No. 2016-0002)		Effectivity Date: Nov. 18, 2020	Expiry Date: Nov 18, 2025

4.1. General procedures on the release of personal data should be

4.1.1. All personal data shall be released only to the data subject pursuant to a lawful purpose and to authorized recipients of such data.

4.1.1.1. Prior to release, DLSMC staff should verify the identity of the person to whom personal data shall be released by asking for a Valid ID. A valid ID should be any ID issued by the government. Expired IDs are not valid forms of identification.

4.1.1.1.1. DLSMC Staff must interview the recipient and verify the identity or establish the relationship with the owner of the personal data or if the recipient is some personnel of a government agency.

4.1.1.2. For Authorized Representative of the owner of the personal data, the following should be presented:

- a. Authorization letter or consent from the owner of the personal data. Authorization letter should contain:
 - i. the name of the person authorized to receive the release of personal data
 - ii. description of the personal data to be released
 - iii. the purpose of requesting the copy of the personal data
 - iv. signature of the personal data owner and the date
- b. Valid ID of the authorized representative
- c. Valid ID of the owner of the personal data
- d. Other valid documents that will establish relationship to the owner of the personal data (ex. If the owner of the personal data is a minor, the personal data shall be released to his or her parents provided that a birth certificate should be presented).


4.1.1.2. The copy of the authorization letter and valid IDs presented should be kept and the *Records Retention and Disposition Schedule* should be applied the same as the retention of the type of record released.

4.1.1.3. Refusal to honor authorization. DLSMC Staff authorized to release personal data will not honor a data subject’s authorization when they have a reasonable doubt or question as to the following information:


- i. Identity of the person presenting the authorization
 - ii. Authenticity of the data subject’s signature
 - iii. Authenticity of the presented valid IDs
2. Refusal to honor authorization must be documented and proper notice to the data subject must be made.

4.1.2. For release of medical records, the following regulations and DLSMC policies applies:

- 4.1.2.1. Policy on Medical Records Safekeeping, Confidentiality, and Authenticity
- 4.1.2.2. General Policies and Procedures on Consolidation, Encoding and Retrieval of Patient’s Data for Healthcare Statistics Report

	Document Name:	Release Date:	Documentation No:
	Data Privacy Manual	Nov. 18, 2020	BPC-PO-19-009-00
	Department:	Version No.: 1.0.0	
	Business Process and Compliance	Page No.: Page 19 of 130	
Regulatory/ Standard Reference: RA 10173 (Data Privacy Act of 2012), Health Privacy Code of the Philippines (AO No. 2016-0002)	Effectivity Date:		Expiry Date:
	Nov. 18, 2020		Nov 18, 2025

- 4.1.2.3. Release of HIV/AIDS test results should adhere to the requirements stated in Article VI, Section 32 of the Republic Act 8504 – “Philippine AIDS Prevention and Control Act of 1998.”
- 4.1.2.4. Release of records pertaining to cases of violence against women and children should adhere to the requirements stated in Section 44 of the Republic Act 9262 – “Anti-Violence Against Women and Their Children Act of 2004.”
- 4.1.2.5. Release of records pertaining to cases of child sexual abuse should adhere to the requirements stated in Presidential Decree No. 603 – “The Child and Youth Welfare Code.”
- 4.1.2.6. Release of records pertaining to cases of drug dependents under voluntary and compulsory submission program should adhere to the requirements stated in Section 60 of the Republic Act 9165 – “Comprehensive Dangerous Drugs Act of 2002.”
- 4.1.2.7. If requested by the data subject’s HMO or Corporate partner for hospital bills payment, consent from the data subject should be acquired prior to release.
- 4.1.2.8. Release of patient data shall only be performed by authorized personnel of the Medical Records Request and Releasing Area.
- 4.1.3. For government agencies, public health authorities, legal representatives, the request for personal data should be made in writing on official letterhead.
- 4.1.4. Release of personal data are allowed without authorization from the data subjects under the following circumstances:
 - a. A court or a party to an action under a valid court order or court subpoena. The valid court order or court subpoena must be signed by a judge.
 - b. Government agencies involved in the payment of fees for medical services rendered to the data subject (ex. Phil health)
 - c. Government agencies if disclosures are required or authorized by law (ex. DOH).
 - d. Qualified personnel for the purpose of management audits, financial audits, program evaluations, but the data subject must not be identified in the audit or program report.
- 4.1.5. Electronic copy of personal data can be released upon the request of the data subject following the *DLSMC’s Email and Communication Policy and Procedure*.
 - 4.1.5.1. Release of personal data using Email, Removable Media (ex. CDs, DVDs), Mobile Phones through Bluetooth communication and messaging applications (ex. Viber, WhatsApp, Messenger, etc):
 - 4.1.5.1.1. If disclosure is done via email the recipient must provide a photo of himself/herself holding a piece of paper with signature over printed name of the requesting party himself/herself.
 - 4.1.5.1.2. Before releasing the personal data, DLSMC Staff should advise the recipient on the risks of confidentiality being breached:
 - a. Risk of the message being intercepted by unauthorized party during transmission.

	Document Name:	Release Date:	Documentation No:
	Data Privacy Manual	Nov. 18, 2020	BPC-PO-19-009-00
	Department:	Version No.: 1.0.0	
	Business Process and Compliance	Page No.: Page 20 of 130	
Regulatory/ Standard Reference: RA 10173 (Data Privacy Act of 2012), Health Privacy Code of the Philippines (AO No. 2016-0002)	Effectivity Date:		Expiry Date:
	Nov. 18, 2020		Nov 18, 2025

b. Risk of the message being sent to wrong email address or unintended recipient.

4.1.5.1.3. Personal data to be released should be encrypted and/or password-protected.

4.1.5.1.4. Password to be used can be the Official Receipt number issued by DLSMC Billing Section after paying for the services availed or nominated by the recipient following the Password Policy and Guidelines of DLSMC.

4.1.5.1.5. Password should be sent separately from the original message if the personal data is to be sent through email.

4.1.5.2. Release of personal data using Portable Media such as USB Storage Device or SD Cards or direct Mobile Phone connection using USB port is strictly prohibited except those where the size of an image/video cannot be sent as an attachment in the email. Hence, released via a USB storage.

4.1.6. Release of personal data by DLSMC staff through facsimile machines is not preferred as this mode of communication is highly unsecured. However, should there be no other means, sending messages through fax should adhere to the *DLSMC’s Email and Communications Policy and Procedure*.

4.1.7. Care must be taken to only release the information which is requested. Do not volunteer information that is not requested.

4.1.8. Sometimes a health record will include information about people other than the patient. Health records should be carefully reviewed before release to check for and remove any third party information in order to avoid a breach of privacy of the third party. Third party personal data contained within a record may be withheld (redacted).


Access

5. Every data subject has the right to reasonable access to his or her personal data being processed by DLSMC.


5.1. Access is granted to the data subject by using a Data Privacy Request Form submitted to the Medical Records Department and to authorized DLSMC personnel and medical staff who have clearance to access and process personal data.

5.1.1. The data subject may request access of the following:

- a. Contents of the data subject’s personal or health data that were processed;
- b. Copy of their Medical Records of any kind subject to the limitations imposed by this privacy manual.
- c. Sources from which personal data were obtained;
- d. Names and addresses of the recipients of the personal data;
- e. Manner by which such data were processed or disclosed;
- f. Reasons for disclosure of personal data to recipients, if there were any;
- g. Information on automated processes where the data will or likely to be made as the sole basis for any decision which would significantly affect the data subject;
- h. Date when the data subject’s data was last accessed and modified; and
- i. Name and address of the Personal Information Controller

	Document Name:	Release Date:	Documentation No:
	Data Privacy Manual	Nov. 18, 2020	BPC-PO-19-009-00
	Department:	Version No.: 1.0.0	
	Business Process and Compliance	Page No.: Page 21 of 130	
Regulatory/ Standard Reference: RA 10173 (Data Privacy Act of 2012), Health Privacy Code of the Philippines (AO No. 2016-0002)		Effectivity Date: Nov. 18, 2020	Expiry Date: Nov 18, 2025

- 5.1.2. Access to documents containing restricted and confidential information shall be accessed only through the use of an Access Request Form subject to the limitations imposed under the Information Classification Policy.
- 5.2. Access to personal data will be limited to only those DLSMC employees authorized to hold, view or handle such information for their current job duties.
- 5.2.1. Restrict access to personal data on a need-to-know basis. (ex. Security personnel may need to know the name and room number of patients to ensure order and safety of the hospital’s patients, personnel and facilities).
- 5.2.2. There should be an Access Control Matrix for all documents or records, and records repositories containing personal data and maintained by the Department-owner of the documents or records.
- 5.2.3. New DLSMC employees should be carefully coached and trained before being allowed to access personal data.
- 5.3. Access to any DLSMC’s electronic Data Processing System must be controlled by login identification and password. Passwords should be in adherence to DLSMC’s Password Policy and Guidelines.
- 5.4. DLSMC personnel who retire, transfer from the Department, end of contract or resign should be removed immediately from mailing lists and access control lists.
- 5.4.1. It is the responsibility of the Department Head to ensure that notification is provided to Human Resources and Information Technology Departments on the personnel movement as soon as reasonably possible.
- 5.5. DLSMC’s Data Center should be in a secured area and have restricted access to authorized DLSMC personnel and service providers.
- 5.5.1. Entrance to the Data Center should remain locked at all times. Entry by authorized personnel should be by means of biometrics machine.
- 5.5.1.1. Only DLSMC IT staff have access or be registered to the Data Center’s biometrics machine.
- 5.5.2. Authorized personnel are only permitted entry to the Data Center in order to undertake specific tasks with respect to the installation, maintenance, auditing and decommissioning of equipment for which they have responsibility.
- 5.5.3. Service Providers must inform DLSMC’s IT Department ahead on their scheduled visit and provide the list of names of their employees and purpose of their visit to the Data Center.
- 5.5.3.1. The Service Provider’s employee/s must log in/out when entering/exiting the Data Center. Entry to the Data Center and should be escorted by DLSMC IT staff.
- 5.5.3.2. Unscheduled visits are not allowed.
- 5.5.4. General entry to the Data Center is not permitted.

	Document Name:	Release Date:	Documentation No:
	Data Privacy Manual	Nov. 18, 2020	BPC-PO-19-009-00
	Department:	Version No.: 1.0.0	
	Business Process and Compliance	Page No.: Page 22 of 130	
Regulatory/ Standard Reference: RA 10173 (Data Privacy Act of 2012), Health Privacy Code of the Philippines (AO No. 2016-0002)		Effectivity Date: Nov. 18, 2020	Expiry Date: Nov 18, 2025


5.5.5. Unauthorized person found in the Data Center should be immediately reported to the Information Technology Department Head for proper action.

5.6. Contractors, consultants and external service providers employed by DLSMC should be subject to strict procedures with regard to accessing personal data by way of Non-Disclosure Agreement in line with the provisions of the DPA.

5.7. At the end of each working day, documents containing personal data should be put in secured locked areas to avoid unauthorized access.

Data Sharing

- 6. Data Sharing shall be allowed when it is expressly authorized by law. Provided, that there are adequate safeguards for data privacy and security, and processing adheres to the principles of Transparency, Legitimate Purpose and Proportionality.
 - 6.1. Data subject must consent to the data sharing even when data is to be shared with an affiliate or mother company, or similar relationships.
 - 6.2. The Data Sharing Agreement does not need prior approval from the NPC. The Data Sharing Agreement shall be subject to review by the NPC, on its own initiative or upon complaint of data subject.
 - 6.3. The data subject shall be provided with the following information prior to collection or before data is shared:
 - a. Identity of the personal information controllers or personal information processors that will be given access to the personal data
 - b. Purpose of data sharing
 - c. Categories of personal data concerned
 - d. Intended recipients or categories of recipient of the personal data
 - e. Existence of the rights of data subjects, including the right to access and correction, and the right to object.
 - f. Other information that would sufficiently notify the data subject of the nature and extent of data sharing and the manner of processing.
 - 6.4. A Data Sharing Agreement is not necessary when the transfer of personal data from one PIC to another is explicitly provided for by existing laws and regulations and protection of personal data is guaranteed. (ex. “AIDSWATCH” under R.A. No 8504 and Philippine National AIDS Council Resolution mandating medical confidentiality and protection of right to privacy of individuals tested or diagnosed with HIV).
 - 6.5. Even when not necessary, it is recommended to enter into a Data Sharing Agreement to ensure accountability of those involved in the Data Sharing, and to better assure personal data protection.
 - 6.6. DLSMC must take reasonable steps to ensure information shared is accurate relevant, up to date, complete and not misleading.
 - 6.7. Data sharing for commercial purposes, including direct marketing, shall be covered by a Data Sharing Agreement.


	Document Name:	Release Date:	Documentation No:
	Data Privacy Manual	Nov. 18, 2020	BPC-PO-19-009-00
	Department:	Version No.: 1.0.0	
	Business Process and Compliance	Page No.: Page 23 of 130	
Regulatory/ Standard Reference: RA 10173 (Data Privacy Act of 2012), Health Privacy Code of the Philippines (AO No. 2016-0002)		Effectivity Date: Nov. 18, 2020	Expiry Date: Nov 18, 2025

Retention

- 7. DLSMC will ensure that personal data under its custody are protected against any accidental or unlawful destruction, alteration and disclosure as well as against any other unlawful processing.
 - 7.1. DLSMC will implement appropriate security measures in retaining collected personal data, depending on the nature of the information.
 - 7.1.1. The personal data is kept for no longer than necessary for the purposes for which the information may lawfully be used.
 - 7.1.2. Retention of personal data shall be allowed in cases provided by law.
 - 7.1.2.1. For medical records, retention should be in accordance with DOH Circular No. 70 s. 1996.
 - 7.1.2.2. For employee records or 201 files, retention should be in accordance with the HR manual on retention of employee data.
 - 7.1.2.3. For accounting records containing personal data, retention should be in accordance with Revenue Regulations No. 17-2013 of the Bureau of Internal Revenue.
 - 7.1.2.4. For CCTV recordings, retention should be in accordance with Quezon City Ordinance No. SP-2139.
 - 7.1.2.5. For other records containing personal data, refer to DLSMC’s Records Retention and Disposition Schedule.
 - 7.1.2.6. Electronic or digital records under the retention period should be password protected or encrypted and backed up whichever is practical.
 - 7.1.2.7. Electronic or digital records can be stored online using Cloud services. Provided that the Cloud service provider should be complying with the requirements of the DPA.
 - 7.1.3. After the lapse of the retention period, all hard and soft copies of personal data shall be disposed and destroyed through secured means. (See **Annex J** of this Manual).
 - 7.1.4. The storage of records under the retention period should be in a secured location that will ensure protection from unauthorized access and disclosure or negligent access.

Disposal

- 8. Personal data shall be disposed or discarded in a secure manner that would prevent further processing, unauthorized access, or disclosure to any other party or the public, or prejudice the interests of the data subjects.
 - 8.1. Paper records containing personal data should be disposed of by shredding or by incineration.
 - 8.1.1. It is recommended to use a cross-cut, diamond cut, or confetti-cut shredder when shredding paper records containing personal data.
 - 8.1.2. No scratch paper shall be recycled for use across DLSMC. All scratch papers at the nursing units must be shredded provided that the documents were reviewed by the Head Nurse.
 - 8.1.3. Actual destruction of paper records containing personal data may be outsourced when there is large volume of records to be destroyed. Provided, that the actual destruction is supervised

	Document Name:	Release Date:	Documentation No:
	Data Privacy Manual	Nov. 18, 2020	BPC-PO-19-009-00
	Department:	Version No.: 1.0.0	
	Business Process and Compliance	Page No.: Page 24 of 130	
Regulatory/ Standard Reference: RA 10173 (Data Privacy Act of 2012), Health Privacy Code of the Philippines (AO No. 2016-0002)		Effectivity Date: Nov. 18, 2020	Expiry Date: Nov 18, 2025

by authorized DLSMC personnel and the service provider signs a Non-Disclosure Agreement and a data sharing agreement.


- 8.1.4. Records containing personal data that is scheduled to be destroyed should be authorized by the Department Head for approval.
- 8.2. Records in soft copy (electronic or digital form) should be permanently deleted.
 - 8.2.1. Use a specialized software (CC Cleaner) to permanently delete specific files.
 - 8.2.2. To delete an entire hard disk drive’s data, perform data wipe using an accredited software application (ex. CC Cleaner).
 - 8.2.2.1. In recycling or reformatting a hard disk drive, perform data wipe before reformatting the drive.
 - 8.2.2.2. When auctioning or donating a workstation, perform a data wipe of the hard disk drive then perform reformat.
 - 8.2.3. For total destruction of the hard disk drive, physically destroy the disc media by:
 - a. Hammering the drive until the disc media is destroyed
 - b. Drilling a hole into the drive and through the disc media
 - c. Cut the disc media into pieces
 - 8.2.4. Destruction of personal data in electronic or digital form stored on a portable storage device (such as USB flash drives) should follow the same procedure when destroying a hard disk drive (refer to 8.2.3.).
 - 8.2.4.1. CDs and DVDs should be physically destroyed by breaking it into many pieces.
 - 8.2.4.2. For older media such as floppy disks and tapes, remove the film and cut it into pieces.

Deletion of personal records in electronic or digital form by a third party service provider is allowed. Provided, that a certificate of destruction should be issued by the third party service provider to DLSMC as evidence of permanent destruction of records at the third party’s premises.

(For disposal of other information classified under the Information Classification Policy see **Annex J**)

Data Quality

- 9. Ensure that all data that is collected, used, or disclosed will be accurate, complete, and up-to-date.
 - 9.1. Personal data should be accurate and where necessary for declared, specified and legitimate purpose, kept up to date.
 - 9.2. Inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted.
 - 9.3. The data subject has the right to dispute the inaccuracy or error in the personal data and have DLSMC correct it immediately and accordingly.
 - 9.3.1. The data subject has the right to correct or update his or her personal data. Request shall only be entertained upon completion of the *Data Privacy Request Form*, which may be filled up by either the patient or any of its authorized representative in proper cases.

	Document Name:	Release Date:	Documentation No:
	Data Privacy Manual	Nov. 18, 2020	BPC-PO-19-009-00
	Department:	Version No.: 1.0.0	
	Business Process and Compliance	Page No.: Page 25 of 130	
Regulatory/ Standard Reference: RA 10173 (Data Privacy Act of 2012), Health Privacy Code of the Philippines (AO No. 2016-0002)		Effectivity Date: Nov. 18, 2020	Expiry Date: Nov 18, 2025


- 9.3.2. The Human Resources Department shall be responsible for requests regarding data rectification of employees.
- 9.3.3. The Medical Records section shall be responsible for requests regarding data rectification of patients by validating such request with the DPO and endorsing the same with the IT Department. The Data Privacy Request Form shall be available in the Medical Records Request and Releasing Area.
- 9.3.4. The IT department shall be responsible in allowing the changing of entries pertaining to the requests regarding data rectification of discharged patients.
- 9.3.5. If the personal data has been corrected, DLSMC shall ensure the accessibility of both the new and the retracted information and the simultaneous receipt of the new and the retracted information by the intended recipients.
- 9.3.6. Recipients or third parties who have previously received such processed personal data shall be informed of its inaccuracy and its rectification, upon reasonable request of the data subject.
- 9.3.7. Out of date or inaccurate personal data should be destroyed once an update was performed. Follow the procedure stated in the Destruction section of this Manual.
- 9.4. The data subject shall have the right to damages or file a complaint with the National Privacy Commission for any damages sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal data, taking into account any violation of the data subject’s rights and freedoms.

V. Security Measures


The security measures shall aim to maintain the confidentiality, integrity and availability of personal data and are intended for the protection of personal data against any accidental or unlawful destruction, alteration, and disclosure, as well as against any other unlawful processing.

Organizational Measures


- 10. A Data Protection Officer will be designated by DLSMC.
 - 10.1. The DPO shall oversee the compliance of DLSMC with the DPA, its IRR, and other related policies, including the conduct of PIA, implementation of security measures, security incident and data breach protocol, and the inquiry and complaints procedure.
 - 10.2. The designation of the DPO comes with the responsibility of providing the DPO the time, resources, and training to effectively perform his or her duty of ensuring that the organization is able to comply with the obligations under the law.
 - 10.3. The DPO should possess specialized knowledge and demonstrate reliability necessary for the performance of his or her duties and responsibilities.
 - 10.3.1. The DPO should have expertise in relevant privacy or data protection policies and practices.
 - 10.3.2. The DPO should have sufficient understanding of the processing operations being carried out by DLSMC, including the information systems, data security and/or data protection needs.

	Document Name:	Release Date:	Documentation No:
	Data Privacy Manual	Nov. 18, 2020	BPC-PO-19-009-00
	Department:	Version No.: 1.0.0	
	Business Process and Compliance	Page No.: Page 26 of 130	
Regulatory/ Standard Reference: RA 10173 (Data Privacy Act of 2012), Health Privacy Code of the Philippines (AO No. 2016-0002)		Effectivity Date: Nov. 18, 2020	Expiry Date: Nov 18, 2025


- 10.4. The DPO should be a full time or regular employee. Where employment is based on contract, the term should be for at least two years.
- 10.4.1. In his or her capacity as DPO, the designated individual may perform (or be assigned to perform) other tasks or assume other functions that do not give rise to any conflict of interest.
- 10.5. The DPO should be empowered to perform his or her functions to assure that DLSMC takes data privacy and security seriously, and must have top management support to allow for meaningful changes in the organization.
- 10.6. The DPO must be independent in the performance of his or her functions, and should be accorded a significant degree of autonomy by DLSMC.
- 10.7. The DPO shall be responsible for structuring, designing and managing the privacy management program, including compliance monitoring, risk assessment, policy and procedure development, capacity building and data subject assistance.
- 10.8. Duties and responsibilities of the Data Protection Officer (see <https://privacy.gov.ph/wp-content/uploads/NPC-Advisory-2017-01-sgd.pdf>)
- 10.9. General obligations of DLSMC relative to the DPO:
- a. Effectively communicate to its personnel, the designation of the DPO and his or her functions;
 - b. Allow the DPO to be involved from the earliest stage possible in all issues relating to privacy and data protection;
 - c. Provide sufficient time and resources (financial, infrastructure, equipment, training, and staff) necessary for the DPO to keep himself or herself updated with the developments in data privacy and security and to carry out his or her tasks effectively and efficiently;
 - d. Grant the DPO appropriate access to the personal data it is processing including the processing systems;
 - e. Where applicable, invite the DPO to participate in meetings of senior and middle management to represent the interest of privacy and data protection;
 - f. Promptly consult the DPO in the event of a personal data breach or security incident; and
 - g. Ensure that the DPO is made a part of all relevant working groups that deal with personal data processing activities conducted inside the organization, or with other organizations.
- 10.10. To ensure that DLSMC personnel, the data subjects, the NPC, or any other concerned party, is able to easily, directly, and confidentially contact the DPO, DLSMC must publish the DPO’s contact details in, at least, the following materials:
- a. Website;
 - b. Privacy notice;
 - c. Privacy policy;
 - d. Privacy manual or privacy guide
- 10.11. For this purpose, the contact details of the DPO should include the following information:
- a. Title or designation
 - b. Postal address
 - c. A dedicated telephone number
 - d. A dedicated email address

	Document Name:	Release Date:	Documentation No:
	Data Privacy Manual	Nov. 18, 2020	BPC-PO-19-009-00
	Department:	Version No.: 1.0.0	
	Business Process and Compliance	Page No.: Page 27 of 130	
Regulatory/ Standard Reference: RA 10173 (Data Privacy Act of 2012), Health Privacy Code of the Philippines (AO No. 2016-0002)		Effectivity Date: Nov. 18, 2020	Expiry Date: Nov 18, 2025

11. Conduct a Privacy Impact Assessment for every processing system of DLSMC involving personal data.
- 11.1. DLSMC is primarily accountable for the conduct of a PIA. This responsibility remains even when it elects to outsource or subcontract the actual conduct of the activity.
- 11.2. PIAs should be performed prior to implementation of new programs, projects, processes or measures that have privacy impacts.
- 11.3. The process takes into account the nature of the personal data to be protected and evaluates the risks to privacy and security represented by the processing of personal data.
- 11.3.1. Conduct of PIA:
- 11.3.1.1. The PIA shall be performed by the DLSMC’s Department Heads in coordination with the DPO and the Privacy Committee members.
- 11.3.1.2. All DLSMC Departments who process personal data should participate in the PIA conduct.
- 11.3.2. Internal or External stakeholders of the personal data processing should be involved when undergoing a PIA. This may be done by active consultation or by including them as participants in the process. Stakeholders may be consulted for specific stages, such as in preparatory stage, during risk analysis and evaluation, or after the process during review that leads up to the preparation of the report.
- 11.4. Any gaps identified in the PIA should be addressed and managed. This might mean implementing new policies and procedures, adapting new systems and technologies entering into outsourcing contracts, or hiring additional personnel.
- 11.5. DLSMC must maintain a record of all its PIA reports. When a report contains information that are privileged or confidential, DLSMC may prepare a PIA summary that can be made available to data subjects upon request.
- 11.6. PIA should be evaluated every year. This does not preclude the conduct of a new PIA on the same data processing system, when so required by significant changes required by law or policy, and other similar circumstances.
- 11.7. A change in law or regulation, or changes within DLSMC requires undertaking a PIA if the changes would affect personal data processing.
- 11.8. In the event a personal data breach occurs, or a complaint is filed by a data subject against DLSMC, the conduct of a PIA shall be considered in evaluating if DLSMC exercised due diligence in the processing of personal data.
- 11.9. When the NPC determines that a processing system of DLSMC poses a significant risk to the rights and freedoms of data subjects, it may request for a copy of the PIA report regarding such system. A copy of the PIA shall be made available to the NPC for compliance monitoring purposes.
12. The Data Processing Systems of the Company are as provided in ANNEX “K”.
13. Duty of Confidentiality of all DLSMC personnel processing personal data must be enforced.
- 13.1. All DLSMC employees will be asked to sign a Non-Disclosure Agreement and a Confidentiality Undertaking during the on-boarding procedure. Attached as Annex B and C respectively.

	Document Name:	Release Date:	Documentation No:
	Data Privacy Manual	Nov. 18, 2020	BPC-PO-19-009-00
	Department:	Version No.: 1.0.0	
	Business Process and Compliance	Page No.: Page 28 of 130	
Regulatory/ Standard Reference: RA 10173 (Data Privacy Act of 2012), Health Privacy Code of the Philippines (AO No. 2016-0002)		Effectivity Date: Nov. 18, 2020	Expiry Date: Nov 18, 2025

- 13.2. All DLSMC employees with access to personal data shall operate and hold personal data under strict confidentiality if the same is not intended for public disclosure.
 - 13.3. Student health professionals, On-the-job trainees, Interns, must sign a Non-Disclosure Agreement and Confidentiality Undertaking and must comply with the DPA and all DLSMC Data Protection and Information Security policies.
 - 13.4. Agencies, sub-contractors or any other organization providing staff augmentation that may have access to, or be involved in the processing of, personal data will be required to complete a NDA.
 - 13.5. It should be noted that DLSMC Staff may only view, access, use, and disclose personal health information when it is necessary for them to do so in order to carry out their work duties.
 - 13.6. If any DLSMC Staff is in doubt as to whether they are permitted to access, use or disclose personal health information, they should seek advice from their respective Manager, Department Head or the DPO.
 - 13.7. All DLSMC employees and personnel shall maintain the confidentiality and secrecy of all personal data that come to their knowledge and possession, even after resignation, termination of contract, or other contractual relations.
14. Develop a Privacy Management Program (PMP) into every major function involving the use of personal data, including product/service development, customer services or public relations initiatives.
 - 14.1. A PMP should proceed from an understanding of the data processing systems within an organization, and should take into account privacy impact assessments and legal obligations and requirements. This should include Privacy Notices and Privacy Policies.
 - 14.2. The PMP should essentially provide a roadmap for compliance with the law.
 - 14.3. A Privacy Notice is not equivalent to consent. Lawful processing done without consent of data subjects should be included in the Privacy Notice.
 - 14.4. Guidelines for the creation of a Privacy Manual is available at <https://privacy.gov.ph/creating-a-privacy-manual/>
 - 14.5. DLSMC should perform the following management of Human Resources
 - a. Conduct a refresher about DPA at least two (2) times a year.
 - b. Maintain a training/seminar about DPA for their DPOs.
 - c. Integrate data privacy into other training programs, such as HR training, information security training and new employee training to streamline important training material into a cohesive training program consistent with its training and communications objectives.
 - d. Provide training/awareness in action to timely issues/topics (e.g. events such as data breaches, violations of the organization’s data privacy policy and new laws or regulations).
 - e. Provide privacy awareness materials (e.g. posters and videos).
 - f. Provide awareness events (e.g. an annual data privacy day/week).
 - g. Require completion of data privacy training as part of the performance review.
 - h. Measure participation in data privacy training activities (e.g. number of participants).
 - 14.6. The DPO should be assured of means to report to DLSMC’s senior management, head of agency.
 - 14.6.1. The DPO shall report on monitoring activities, PIA reports, audits, security assessments, breach management, complaints and the exercise of data subject’s rights.

	Document Name:	Release Date:	Documentation No:
	Data Privacy Manual	Nov. 18, 2020	BPC-PO-19-009-00
	Department:	Version No.: 1.0.0	
	Business Process and Compliance	Page No.: Page 29 of 130	
Regulatory/ Standard Reference: RA 10173 (Data Privacy Act of 2012), Health Privacy Code of the Philippines (AO No. 2016-0002)		Effectivity Date: Nov. 18, 2020	Expiry Date: Nov 18, 2025

14.7. Capacity Building is needed as part of DLSMC’s preventive measures against personal data breach.

14.7.1. Orientation or training programs for DLSMC employees, regarding privacy or security policies should be conducted.

14.7.2. DLSMC employees who handle personal data directly may need additional training specifically tailored to their roles.

14.7.3. DLSMC shall sponsor a mandatory training on data privacy and security at least once a year.

14.7.3.1.DLSMC management shall ensure attendance and participation of their personnel in relevant trainings and orientations, as often as necessary.

- 14.7.3.2. For personal data protection training and education to be effective, it should:
- a. Be given to new employees and periodically thereafter (at least once a year);
 - b. Cover the policies and procedures established by DLSMC;
 - c. Be delivered in an appropriate and effective manner, based on organizational needs;
 - d. Circulate essential information to relevant employees as soon as practical if an urgent need arises.

13.8. Continuing assessment and revision of DLSMC’s PMP, Data Privacy policies and procedure should be established.

13.8.1. In order to properly protect personal data and meet legal obligations, DLSMC should monitor, assess and revise its privacy management framework to ensure it remains relevant and effective.


13.8.1.1. DLMSC to develop an Oversight and Review Plan to help keep its PMP on track and up-to-date.

13.8.1.1.1. The DPO should monitor data processing systems and ensure conduct of PIAs when necessary.

13.8.1.1.2. The DPO should develop and oversight and review plan on a periodic basis that sets out how and when the PMP’s effectiveness will be monitored and assessed.

13.8.1.2. The effectiveness of program controls should be monitored, periodically audited, and where necessary, revised.

- 13.8.1.2.1. Monitoring, an ongoing process, should address the following questions:
- a. What are the latest threats and risks?
 - b. Are the program controls addressing new threats and reflecting the latest compliant or audit findings, or guidance of the NPC?
 - c. Are new services being offered that involve increased collection, use or disclosure of personal data?
 - d. Is training necessary? If yes, is it taking place? Is it effective? Are policies and procedures being followed? And, Is the training program up to date?

	Document Name:	Release Date:	Documentation No:
	Data Privacy Manual	Nov. 18, 2020	BPC-PO-19-009-00
	Department:	Version No.: 1.0.0	
	Business Process and Compliance	Page No.: Page 30 of 130	
Regulatory/ Standard Reference: RA 10173 (Data Privacy Act of 2012), Health Privacy Code of the Philippines (AO No. 2016-0002)		Effectivity Date: Nov. 18, 2020	Expiry Date: Nov 18, 2025

13.8.2. The policies for data privacy should include procedures for documentation, regular review, evaluation, and updating of the privacy and security policies and practices in the organization.

13.8.3. If problems are found during the monitoring process, concerns will need to be documented and addressed by the appropriate department. Critical issues should be brought to the attention of the top management.

13.8.4. DPO should conduct periodic assessments to ensure key processes are being respected.

13.8.4.1. Periodic assessments or internal audit should be conducted at least once a year. This could include the form of customer and employee feedback.

13.8.4.2. Third Party audit or external audit should be conducted by accredited third party service provider to DLSMC to assess compliance to the DPA at least once a year.

13.8.4.3. These assessments should adhere to DLSMC’s *Data Privacy Review and Audit Procedure*.

13.8.4.4. DPO should perform or monitor the third party assessors with whom DLSMC shares personal data of its patients or employees using the Data Sharing Agreement.

13.8.5. DLSMC’s PMP should be regularly assessed and revised, taking into account PIAs, effectiveness of implementation, and data privacy best practices.

13.8.5.1. The PMP should be assessed once every year and covers all PIA and policies for data protection and information security.

13.8.5.2. This assessment should be initiated by the DPO and in collaboration with all process owners/Department Head.

13.8.5.3. Evidence of the assessment must be documented and action items identified should be tracked to closure.

14. Review of Privacy Manual

14.1. This Manual shall be reviewed and evaluated annually in conjunction with the assessment of DLSMC’s Privacy Management Program.


14.2. Privacy and security policies and practices within the organization shall be updated to remain consistent with current data privacy best practices.

Physical Measures

15. DLSMC shall apply physical measures to protect personal data from physical actions and events that could cause serious loss or damage. This includes protection from natural disasters (such as fire, flood), power disturbances and external access (e.g. burglary, theft, prying eyes) and other similar physical threats.

15.1. Format of personal data to be collected by DLSMC from data subject may be in digital/electronic format and paper-based/physical format.

15.2. Storage type and location for the personal data in the custody of DLSMC should be secured.

	Document Name:	Release Date:	Documentation No:
	Data Privacy Manual	Nov. 18, 2020	BPC-PO-19-009-00
	Department:	Version No.: 1.0.0	
	Business Process and Compliance	Page No.: Page 31 of 130	
Regulatory/ Standard Reference: RA 10173 (Data Privacy Act of 2012), Health Privacy Code of the Philippines (AO No. 2016-0002)		Effectivity Date: Nov. 18, 2020	Expiry Date: Nov 18, 2025

15.2.1. All personal data being processed by DLSMC shall be stored in a secured room, where paper-based documents may be kept in locked filing cabinets.

15.2.1.1. Secured storage room should have sturdy doors with door locks.

15.2.1.1.1. Keys to the door locks must be handled by DLSMC personnel authorized to maintain the storage room.

15.2.1.4.2. Offices and personal data storage areas that are unattended should be locked.

15.2.1.4.3. The temperature, humidity and lighting of the storage room should be adequate to avoid having the paper-based documents damaged by discoloration or contamination or by insect infestation.

15.2.1.3. DLSMC may store inactive/older paper-based documents containing personal data in a secure off-site storage facility. Provided, that the service provider should have adequate means to secure DLSMC’s paper records and abides by the requirements set forth in the DPA.

15.2.1.4.1. In this case, paper-based documents that are required frequently should be stored in-site, while paper-based documents that are needed to be retained for legal or other reasons should be stored off-site or in a secured location monitored by an authorized person and the Data Protection Officer

15.2.1.4.2. When the retention period of paper-based documents stored off-site has lapse, these documents should be destroyed following the procedure stated in the Destruction section of this Manual.

15.2.1.4.3. A Data Sharing Agreement shall be enforced between DLSMC and the service provider if the former decides to outsource the storage of its manual files.

15.2.1.4. There should be enough space to access files without difficulty.

15.2.1.5. Boxes and files should never overhang shelves.

15.2.1.6. Records should not be stored on the top of shelving units, as these will be too close to lighting, and exposed to possible water damage from fire sprinklers, as well as making storage units unstable.


15.2.1.7. Storage boxes, where used, should not be stacked more than four boxes high, should not be stored in corridors, and should not block or restrict access to doors, stairways, or office areas.

15.2.2. Personal data in digital/electronic form should be stored in workstations or storage devices provided and installed by DLSMC.


15.2.2.1.DLSMC employees are provided with workstations or electronic gadgets that are needed in performing their duties. Prior to the issuance of the workstations or electronic gadgets, the employee must sign the *Confidentiality Undertaking Form*.

15.2.2.2.Workstations provided should have an installed anti-virus software.


15.2.2.3.The network that the workstations connect to must be protected by a firewall.

	Document Name:	Release Date:	Documentation No:
	Data Privacy Manual	Nov. 18, 2020	BPC-PO-19-009-00
	Department:	Version No.: 1.0.0	
	Business Process and Compliance	Page No.: Page 32 of 130	
Regulatory/ Standard Reference: RA 10173 (Data Privacy Act of 2012), Health Privacy Code of the Philippines (AO No. 2016-0002)		Effectivity Date: Nov. 18, 2020	Expiry Date: Nov 18, 2025

- 15.2.2.4. Workstations processing personal data should have physical security measures employed. Active-Directory driven access and screen locks must be enabled on such device/s or equipment.
- 15.2.2.5. Laptops must be kept in a locked cabinet at the end of work hours.
- 15.2.2.6. Care should be taken when bringing laptops outside DLSMC. It is the user’s responsibility to take appropriate precautions to prevent loss, theft, and/or damage to their assigned laptops and information stored on it.
 - 15.2.2.4.1. Only connect to trusted and secure wireless networks.
 - 15.2.2.4.2. Do not leave the laptop in an unattended vehicle.
 - 15.2.2.4.3. In case of loss or theft, the user should report the case immediately to the IT Department within 24 hours.
 - 15.2.2.4.3.1. IT Department should disconnect the lost device from DLSMC’s email and file systems.
- 15.2.2.5. Portable storage media (ex. USB Flash Drives, CDs, DVDs) should only be used for data transfer where there is a business requirement to do so, should only be used on approved workstations and must only contain password protected files.
- 15.2.2.6. The IT department shall grant access to the use of flash drive only for legitimate business purposes. Any transfer of files from any of the device or to any device must be reviewed and granted only by the IT Department with documented request from the device owner.
- 15.3. Access procedure for personal data storage room must be observed by DLSMC personnel.
 - 15.3.2. Only authorized personnel shall be allowed inside the secured storage room. Other personnel may be granted access to the room to perform contracted duties (e.g. security, housekeeping, maintenance) but should be supervised to avoid theft and unauthorized access to personal data.
 - 15.3.3. Access Control Policy should be implemented to prevent unauthorized access to any form of personal data.
 - 15.3.4. Physical access to DLSMC’s servers and network equipment is highly restricted to DLSMC’s IT staff or to authorized personnel.
 - 15.3.5. Only those with a true business need should be able to access the secured personal data storage room.
 - 15.3.6. Further personal data access procedure is found in the Access section (5) of this Manual.
- 15.4. Monitoring and limitation of access to secured personal data storage room or facility shall be in effect.
 - 15.4.2. All personnel authorized to enter and access the secured personal data storage room or facility may be monitored through the outsourced Security personnel via physical check or via the installed CCTV security cameras.
 - 15.4.2.1. 24-hour security is employed by DLSMC to secure the areas where the offices and personal data storage rooms are located.

	Document Name:	Release Date:	Documentation No:
	Data Privacy Manual	Nov. 18, 2020	BPC-PO-19-009-00
	Department:	Version No.: 1.0.0	
	Business Process and Compliance	Page No.: Page 33 of 130	
Regulatory/ Standard Reference: RA 10173 (Data Privacy Act of 2012), Health Privacy Code of the Philippines (AO No. 2016-0002)		Effectivity Date: Nov. 18, 2020	Expiry Date: Nov 18, 2025


- 15.4.3. Challenge unauthorized persons who enter personal data processing areas.
- 15.5. Design of office space/work station should consider privacy enough to ensure protection against unauthorized or negligent disclosure.
- 15.5.2. The workstations are positioned with considerable spaces between them to maintain privacy and protect the processing of personal data.
- 15.5.3. The workstations should not be positioned where unauthorized persons can easily see the monitor.
- 15.5.4. Design of office space and work stations, including the physical arrangement of furniture and equipment, shall provide privacy to anyone processing personal data, taking into consideration the environment and accessibility to the public.
- 15.5.4.1. Applicants filling-out application forms and in the Application Form Kiosk must be isolated and free from prying eyes or where personal data may be stolen by use of any image-capturing devices. Similarly, on-boarding employees should be given the same privacy setting.
- 15.5.4.2. In-patients filling-out the Patient Admission Form should be accorded privacy to avoid personal data being disclosed to unauthorized persons in the area.
- 15.5.4.3. Out-patients filling-out forms on DLSMC’s Out-Patient or Ancillary stations should be given sufficient privacy to avoid their personal data being disclosed to unauthorized persons within the area.
- 15.6. DLSMC personnel involved in processing, and their duties and responsibilities should be defined.
- 15.6.2. Persons involved in processing shall always maintain confidentiality and integrity of personal data.
- 15.6.2.1. They should be trained on the Data Privacy requirements and be coached prior to processing personal data.
- 15.6.2.2. Refer to the Duty of Confidentiality section (12) of this Manual.
- 15.7. Modes of transfer of personal data within the organization, or to third parties must ensure security to avoid being stolen.
- 15.7.2. Paper-based personal data should be transported in a way that mitigates the risks of theft, loss, or disclosure.
- 15.7.2.1. Ensure that the person transporting the personal data is authorized and will observe proper confidentiality of the personal data and is aware on the requirements of the DPA.
- 15.7.2.2. Enclose paper-based personal data in an envelope to avoid negligent or unauthorized disclosure and to reduce the risk of dropping or losing the document.
- 15.7.3. Transfer of personal data in electronic form should ensure security through the use of password protection.

	Document Name:	Release Date:	Documentation No:
	Data Privacy Manual	Nov. 18, 2020	BPC-PO-19-009-00
	Department:	Version No.: 1.0.0	
	Business Process and Compliance	Page No.: Page 34 of 130	
Regulatory/ Standard Reference: RA 10173 (Data Privacy Act of 2012), Health Privacy Code of the Philippines (AO No. 2016-0002)		Effectivity Date: Nov. 18, 2020	Expiry Date: Nov 18, 2025

- 15.7.3.1. Transfer of personal data via electronic mail shall use a secure email facility. All document sent across via electronic mail shall be password protected including any or all attachments.
- 15.7.3.2. Password protection is required when files are being transported using mobile storage devices, such as Flash Drive/s.
- 15.7.3.3. Facsimile technology, as much as possible, shall not be used for transmitting documents containing personal data.

Technical Measures

- 16. DLSMC must implement technical security measures to make sure that there are appropriate and sufficient safeguards to secure the processing of personal data, particularly the computer network in place, including encryption and authentication processes that control and limit access.
 - 16.1. Monitoring for Security Breaches must be established.
 - 16.1.1. DLSMC IT Department shall use a system to monitor security breaches and alert the organization of any attempt to interrupt or disturb the system.
 - 16.1.1.1. This system should be able to determine the following:
 - a. Unusual bandwidth traffic
 - b. Presence of unknown or unauthorized IP addresses on wireless networks
 - c. Multiple failed login attempts for system authentication and event logs
 - d. Suspicious activity on the network after-hours
 - e. Unexplained system reboots or shutdowns
 - f. Services and applications configured to launch automatically without authorization
 - g. Unusually slow internet or devices
 - h. Account access and password changes
 - i. Abnormal administrative user activity
 - 16.1.2. In case of a confirmed security breach, the Breach and Security Incident section of this Manual will apply.
 - 16.2. Security features of the software and application/s used must be evaluated prior to deployment.
 - 16.2.1. DLSMC IT Department shall first review and evaluate software applications before the installation thereof in computers and devices of the organization to ensure the compatibility of security features with overall operations.
 - 16.2.1.1. Use of the software or application/s does not interfere, preclude, or circumvent anti-virus controls of the end-user device, server or network.
 - 16.2.1.2. The software or application/s does not require privileged access on end-user devices to function.
 - 16.2.2. DLSMC IT Department should keep abreast of the latest software patches and deploy the fix as soon as it is tested and validated that the fix has no bugs that can cause operational issue to the Hospital systems (ex. monthly Windows Operating System security update).

	Document Name:	Release Date:	Documentation No:
	Data Privacy Manual	Nov. 18, 2020	BPC-PO-19-009-00
	Department:	Version No.: 1.0.0	
	Business Process and Compliance	Page No.: Page 35 of 130	
Regulatory/ Standard Reference: RA 10173 (Data Privacy Act of 2012), Health Privacy Code of the Philippines (AO No. 2016-0002)		Effectivity Date: Nov. 18, 2020	Expiry Date: Nov 18, 2025

16.3. Process for regularly testing, assessment and evaluation of effectiveness of security measures should be performed by DLSMC.

16.3.1. DLSMC shall review security policies conduct vulnerability assessments and perform penetration testing within the company at least once a year.

16.3.1.1. Data Protection and Information Security Policies should be audited internally by the DPO and externally by an accredited third party assessor at least once a year.

16.3.1.1.1. This practice should determine if Data Protection and Information Security policies are being followed as intended and is still appropriate to the DLSMC’s processes.

16.3.1.1.2. If discrepancies are found, or the policies are no longer applicable as written, these policies must be changed to fit DLSMC’s current requirements and the DPA requirements.

16.3.1.1.3. Prior to the start of external assessment, the third party assessor must sign a Data Sharing Agreement.

16.3.1.2. Vulnerability Assessment and Pen-Testing is required to be conducted by a qualified third party service provider.

16.3.1.2.1. All devices connected to DLSMC’s network are subject to security vulnerability assessment and pen-testing.

16.3.1.2.2. Due to the intrusive nature of a pen-testing, and to better manage risks associated with such tests, a signed NDA is required prior to commencing the pen-testing

16.3.1.2.3. High risk issues must be remediated in a timely manner by affected DSLMC Departments and implement compensating controls to reduce risks highlighted in the report.


16.3.1.2.4. Care must be taken when Pen-Testing is to be performed as it intentionally attacks the network in finding security weaknesses which may result to a damaged network or system. It is suggested that Pen-Testing be performed in a non-production setting or in a staging environment.

16.4. Policies and procedures relating to encryption, authentication process, and other technical security measures that control and limit access to personal data should be implemented.

16.4.1. DLSMC is responsible for securing strategic and operational control of its hardware, software and telecommunication facilities. Included in this mandate is the implementation of effective safeguards and firewalls to prevent unauthorized access to system processes and computing or telecommunication operational centers.

16.4.2. *DLSMC Information Security Policy* represents the minimum requirements for information security at DLSMC. The policy includes:


- a. Acceptable Use Policy
- b. Email and Communication Policy
- c. Network Security Policy
- d. Internet Access Policy

	Document Name:	Release Date:	Documentation No:
	Data Privacy Manual	Nov. 18, 2020	BPC-PO-19-009-00
	Department:	Version No.: 1.0.0	
	Business Process and Compliance	Page No.: Page 36 of 130	
Regulatory/ Standard Reference: RA 10173 (Data Privacy Act of 2012), Health Privacy Code of the Philippines (AO No. 2016-0002)		Effectivity Date: Nov. 18, 2020	Expiry Date: Nov 18, 2025


- e. BYOD Policy
- f. Encryption Policy
- g. Password Policy and Guidelines
- h. Authentication Policy
- i. Backup Policy
- j. Data Classification Policy
- k. Guest Access Policy
- l. Wireless Access Policy
- m. Third Party Connection Policy

VI. Breach and Security Incidents


17. DLSMC should implement policies and procedures for the management of a personal data breach, including security incidents.
- 17.1. The creation of a Data Breach Response Team (DBRT) will lead DLSMC in handling security incidents or personal data breach.
- 17.1.1. The DBRT shall be responsible for ensuring immediate decision regarding critical action in the event of a security incident or personal data breach. The team may include the DPO.
- 17.1.1.1.DLSMC’s Data Breach Response Team are as provided in Annex “I”.
- 17.1.2. The team shall conduct an initial assessment of the incident or breach in order to ascertain the nature and extent thereof.
- 17.1.3. The team shall be responsible for the following:
- a) Implementation of the security incident management policy of the personal information controller or personal information processor;
 - b) Management of security incidents and personal data breaches; and
 - c) Compliance by the personal information controller or personal information processor with the relevant provisions of the DPA, its IRR, and all related issuances by the Commission on personal data breach management.
- 17.1.4. The team shall also assess and evaluate a security incident, restore integrity to the information and communications system, mitigate and remedy any resulting damage, and comply with reporting requirements.
- 17.1.5. It shall also execute measures to mitigate the adverse effects of the incident or breach (see 17.2).
- 17.1.6. Responsibilities of the DBRT can be found in the *Security Incident Management Policy and Procedure*.
- 17.1.7. Functions of the DBRT may be outsourced.
- 17.1.5.1 Such outsourcing shall not reduce the requirements found in the DPA.
- 17.1.5.2 The DPO shall remain accountable for compliance with applicable laws and regulations

	Document Name:	Release Date:	Documentation No:
	Data Privacy Manual	Nov. 18, 2020	BPC-PO-19-009-00
	Department:	Version No.: 1.0.0	
	Business Process and Compliance	Page No.: Page 37 of 130	
Regulatory/ Standard Reference: RA 10173 (Data Privacy Act of 2012), Health Privacy Code of the Philippines (AO No. 2016-0002)		Effectivity Date: Nov. 18, 2020	Expiry Date: Nov 18, 2025

- 17.1.6 In cases where the DPO is not part of the DBRT, the DBRT shall submit a written report addressed to the DPO detailing the actions taken.
- 17.2. DLSMC should implement measures to prevent and minimize occurrence of breach and security incidents.
- 17.2.1. DLSMC shall regularly conduct the following activities that will prevent security incident or personal data breach:
- a. Privacy Impact Assessment to identify risks in the processing system
 - b. Monitor for security breaches
 - c. Annual Vulnerability Scanning and Pen Testing of computer networks
 - d. Personnel directly involved in the processing of personal data must attend trainings and seminars for capacity building at least once a year
 - e. Periodic review of policies and procedures being implemented in DLSMC
 - f. Data governance: Identify data sources, inventory sensitive data, and map locations
 - g. Create an incident response policy to contain security incidents and restore system integrity
 - h. Plan a mitigation method that will address possible harm and negative consequences on data subjects in the event of a breach
 - i. Conduct a self-audit plan to include data security and compliance assessments
 - j. Formulate a data retention and data destruction policy
 - k. Regularly update back-up or restoration systems for reference comparison of personal data
- 17.3. DLSMC shall establish a procedure for the recovery and restoration of personal data.
- 17.3.1. DLSMC shall always maintain a backup file for all personal data under its custody.
- 17.3.2. In the event of a security incident or personal data breach, it shall always compare the backup with the affected file to determine the presence of any inconsistencies or alterations resulting from the incident or breach.
- 17.3.3. Refer to the *Security Incident Management Policy and Procedure* for the recovery and restoration procedure.
- 17.4. A notification protocol should be applied by DLSMC should there be instances of personal data breach or security incident.
- 17.4.1. The Head of the DBRT shall inform the management of the need to notify the NPC and the data subjects affected by the incident or breach within the period prescribed by law. Management may decide to delegate the actual notification to the head of the DBRT.
- 17.5. The DBRT shall prepare a detailed documentation of every security incident or personal data breach encountered, as well as an annual report, to be submitted to the management and the NPC, within the prescribed period.
- 17.5.1. All actions taken by DLSMC shall be properly documented. Reports should include:
- a. Description of the personal data breach, its root cause and circumstances regarding its discovery;
 - b. Actions and decisions of the DBRT
 - c. Outcome of the breach management, and difficulties encountered; and

	Document Name:	Release Date:	Documentation No:
	Data Privacy Manual	Nov. 18, 2020	BPC-PO-19-009-00
	Department:	Version No.: 1.0.0	
	Business Process and Compliance	Page No.: Page 38 of 130	
Regulatory/ Standard Reference: RA 10173 (Data Privacy Act of 2012), Health Privacy Code of the Philippines (AO No. 2016-0002)		Effectivity Date: Nov. 18, 2020	Expiry Date: Nov 18, 2025

- d. Compliance with notification requirements and assistance provided to affected data subjects.
- 17.6. The NPC and affected data subjects should be notified of the personal data breach within seventy-two (72) hours from knowledge of the breach, unless there is a reason to postpone or omit notification, subject to approval of the NPC.
- 17.6.1. The NPC must be notified based on available information even if the full extent of the breach is not yet known.
- 17.6.2. The NPC must be notified if the personal data breach involves at least 100 data subjects or the disclosure of sensitive personal information will harm data subjects.
- 17.6.3. In other cases, notification may be delayed if the scope of the breach cannot be determined within the 72-hour period, or if it is necessary to prevent further disclosure or to restore system integrity.
- 17.7. Full report to NPC must be submitted by DLSMC within five (5) days upon knowledge or when there's a reasonable belief that a personal data breach has occurred, unless granted additional time by the NPC.
- 17.7.1. The following security breach are subject to the notification requirements:
- a. Involves sensitive personal information, or information that may be used to enable identity fraud.
 - b. There is reason to believe that information has been acquired by an unauthorized person.
 - c. The unauthorized acquisition is likely to give rise to a real risk of serious harm.
- 17.7.2. When there is doubt as to the need to notify, consider if it:
- a. Would likely affect national security, public safety, public order, or public health
 - b. Involves at least 100 individuals
 - c. Are required by laws or rules to be confidential
 - d. Pertain to vulnerable groups
- 17.7.3. In general, the contents of notification to NPC are as follows:
- a. Nature, extent and impact of the breach
 - b. Sensitive personal information possibly involved
 - c. Measures taken by DLSMC to address the breach
 - d. Details of the DPO or contact person designated by DLSMC for more information
 - e. Any assistance to be provided to the affected data subject
- 17.7.4. In general, the contents of notification to affected data subjects is the same contents as notification of NPC but must include instructions on how the data subjects will get further information and recommendations to minimize risks resulting from breach.
- 17.7.5. NPC may be notified by either written (see 18.4) or electronic means (complaints@privacy.gov.ph) but DLSMC must have confirmation that the notification has been received.
- 17.7.6. Affected data subjects shall be notified individually, by written or electronic means, unless allowed by NPC to use alternative means.
- 17.7.7. DLSMC should cooperate with the NPC where there is an investigation related to the breach.

	Document Name:	Release Date:	Documentation No:
	Data Privacy Manual	Nov. 18, 2020	BPC-PO-19-009-00
	Department:	Version No.: 1.0.0	
	Business Process and Compliance	Page No.: Page 39 of 130	
Regulatory/ Standard Reference: RA 10173 (Data Privacy Act of 2012), Health Privacy Code of the Philippines (AO No. 2016-0002)	Effectivity Date:		Expiry Date:
	Nov. 18, 2020		Nov 18, 2025

17.7.8. DLSMC should document all security incidents and must submit an annual report to the NPC at reports@privacy.gov.ph

VII. Inquiries and Complaints

18. Data subjects may inquire or request for information regarding any matter relating to the processing of their personal data under the custody of DLSMC, including the data privacy and security policies implemented to ensure the protection of their personal data.

18.1. Data subjects may submit a complaint or inquiry relating to DLSMC’s Data Privacy policies and procedures to:

Data Privacy Office
 DE LOS SANTOS MEDICAL CENTER
 201 E. Rodriguez Sr. Blvd. Quezon City, Philippines 1112
 Tel. No.: +63 2 893 5762 (89-DLSMC) ext. 8828 or +63 2 877 8828
 Mobile No.: +63 9357004157
 Email Address: privacy@dlsmc.ph

18.2. In the event that a privacy complaint is received by DLSMC, the *Data Privacy Inquiries and Complaints Procedure* will apply.

18.2.1. The *Data Privacy Complaint Form* is found in the **Annex** section of this Manual.

18.3. The DPO will be responsible in managing or providing advice to concerned DLSMC department regarding inquiries or complaints about data privacy.


18.4. If the complainant is not satisfied with the outcome of the investigation, the data subject may make a complaint to the NPC:

National Privacy Commission
 5th Floor, Delegation Building, PICC Complex,
 Roxas Boulevard, Pasay City, Metro Manila, Philippines
 Mobile Phone: +63 945 1534299; +63 939 9638715
 Tel. No. 8234-2228
 Email: complaints@privacy.gov.ph

18.5. Should the complaint be verified as a reportable breach, the Breach and Security Incidents section of this Manual shall apply.

VIII. Effectivity

The provisions of this Manual are effective this 18th day of November, 2020, until revoked or amended by DLSMC’s Data Privacy Officer.

	Document Name:	Release Date:	Documentation No:
	Data Privacy Manual	Nov. 18, 2020	BPC-PO-19-009-00
	Department:	Version No.: 1.0.0	
	Business Process and Compliance	Page No.: Page 40 of 130	
Regulatory/ Standard Reference: RA 10173 (Data Privacy Act of 2012), Health Privacy Code of the Philippines (AO No. 2016-0002)		Effectivity Date: Nov. 18, 2020	Expiry Date: Nov 18, 2025

IX. References

Republic Act 10173 - Data Privacy Act of 2012, <https://privacy.gov.ph/data-privacy-act/#11>

Implementing Rules and Regulations of the Data Privacy Act of 2012, <https://privacy.gov.ph/implementing-rules-regulations-data-privacy-act-2012/>

NPC Privacy Toolkit – A guide for Management and Data Protection Officers, 2nd edition

Summary: Philippines Data Privacy Act and implementing regulations, <https://iapp.org/news/a/summary-philippines-data-protection-act-and-implementing-regulations/>

Data Privacy Act, Ivy D. Patdu, National Privacy Commission, May 29, 2017

Republic Act 9262 – Confidentiality of records pertaining to cases of violence against women and children, “Anti-Violence against Women and their Children Act of 2004”

Republic Act 8504 – Medical confidentiality of HIV cases, “Philippine AIDS Prevention and Control Act of 1998”

Republic Act 603 – Confidentiality of records of child sexual abuse, “The Child and Youth Welfare Code”

Republic Act 9165 – Confidentiality of records of drug dependents under Voluntary and Compulsory Submission program, “Comprehensive Dangerous Drugs Act of 2002”

DOH Circular 70 s. 1996 – Revised Disposition Schedule of Medical Records

NSW Health Privacy Manual for Health Information, <http://www.health.nsw.gov.au/policies/manuals/Pages/privacy-manual-for-health-information.aspx>


Fax machine security: Creating a corporate faxing policy, <http://www.computerweekly.com/tip/Fax-machine-security-Creating-a-corporate-faxing-policy>

Health Point Release of Medical Records Policy & Procedure, <http://www.bvcaa.org/HSP/Administrative%20P&P/Medical%20Records/Release%20of%20Medical%20Records%208.16.pdf>

Personal Record Retention and Destruction Plan, <https://www.privacyrights.org/consumer-guides/personal-data-retention-and-destruction-plan>

X. Annexes

- Annex A- DATA PRIVACY CONSENT FORM FOR EMPLOYEES
- Annex B - CONFIDENTIALITY UNDERTAKING FORM
- Annex C - DATA PRIVACY REQUEST FORM
- Annex D - RECORDS DISPOSAL FORM
- Annex E - PERSONAL DATA BREACH REPORT FORM
- Annex F - WEBSITE DATA PRIVACY NOTICE
- Annex G - DATA SHARING AGREEMENT
- Annex H - DATA PRIVACY COMPLAINTS AND INQUIRIES PROCEDURE

	Document Name:	Release Date:	Documentation No:
	Data Privacy Manual	Nov. 18, 2020	BPC-PO-19-009-00
	Department:	Version No.: 1.0.0	
	Business Process and Compliance	Page No.: Page 41 of 130	
Regulatory/ Standard Reference: RA 10173 (Data Privacy Act of 2012), Health Privacy Code of the Philippines (AO No. 2016-0002)		Effectivity Date: Nov. 18, 2020	Expiry Date: Nov 18, 2025

- Annex I - SECURITY INCIDENT RESPONSE POLICY AND PROCEDURE
- Annex J - INFORMATION CLASSIFICATION POLICY
- Annex K - RECORDS RETENTION AND DISPOSITION SCHEDULE
- Annex L - DATA PROCESSING SYSTEMS INVENTORY
- Annex M - DATA PRIVACY PENALTIES FOR VIOLATIONS

XI. CHANGE LOG

REV NO.	CREATION DATE	PAGE REVISED	REVISION HISTORY
00	November 18, 2020	0	New Creation



DATA PRIVACY CONSENT FORM FOR EMPLOYEES

In the course of your employment, De Los Santos Medical Center will process Personal Information and Sensitive Personal Information relating to you. Such processing of Personal Information may include its collection, recording, updating, access, modification, retrieval, use, retention and disposal. These Personal Information include information which may be used for identification purposes, other personal circumstances, contact information, your educational and medical background.

In signing this consent form, you provide consent to:

- 1. The processing of your Personal Information, as provided under applicable laws, regulations, and De Los Santos Medical Center's policies, for its and its affiliates', related entitles', and partners' legitimate purposes, including, but not limited to, payroll, labor union, and other company-related matters pertaining to recruitment, employee movements and separation.
- 2. Making your Personal Information available to De Los Santos Medical Center's affiliates, related entities, and partners for them to process the Personal Data for their own benefit, for the same purposes as indicated above. List of our affiliates and partners is available at the HR department.
- 3. The disclosure of your Personal Information to De Los Santos Medical Center's affiliates, related entities, and partners, and to permit De Los Santos Medical Center's affiliates, related entities, and partners also to make your Personal Data available:
 - a. To third parties who provide products or services to De Los Santos Medical Center's affiliates, related entities, and partners for the same purposes as described above; and
 - b. To other third parties, where required or permitted by law, including regulatory authorities, government agencies, as well as parties with whom you voluntarily transact.

You also warrant that, before providing us with the Personal Information of your parents/guardian (your contacts, for brevity), you have obtained their consent to: (I) you collecting their Personal Information; (ii) you sharing the same with De Los Santos Medical Center's affiliates, related entitles, and partners, and the third parties as indicated above; and (lit) to the processing (for the same purpose's as described above) of their Personal Information by De Los Santos Medical Center's affiliates, related entities, and partners indicated above as provided herein.

The Personal Information you provide will be retained by De Los Santos Medical Center during your employment with us and for a period of 5 years effective upon separation from DLSMC regardless of the nature of separation for the purpose of employment verification. Unless retention for a longer period is required for reasonable cause, the Personal Information shall, upon the lapse of the Personal Data Retention Period, be disposed of by De Los Santos Medical Center in accordance with applicable laws and regulations.

You and your contacts are entitled to certain rights in relation to the Personal Information that may be collected from you (and from your contacts), including the right to access, correction, and to object to the processing, as well as the right to file a complaint before the National Privacy Commission in case of violation of your or your contacts' rights as data subjects. You may consult the De Los Santos Medical Center's Data Protection Officer at privacy@dismc.ph or at 889-35762 loc. 8828 for any concerns regarding your Personal Data.

Signature Over Printed Name

Date



CONFIDENTIALITY UNDERTAKING FORM

I, _____, hereby state that I am currently employed/affiliated as a/an _____ of Delos Santos Medical Center (DLSMC), with principal office at 201 E Rodriguez Sr. Ave, Quezon City, 1112 Metro Manila;

As an employee/affiliate of DLSMC, who controls the collection, holding/storage, processing or use including disclosure and disposal of personal data or personal information (PI), sensitive personal information (SPI) including privileged information, pertaining to DLSMC employees and its data subjects, as stated in our Privacy Policy pursuant to the provisions of the Data Privacy Act of 2012 (Republic Act No. 10173) and its Implementing Rules and Regulations (IRR), which designation, include attendant duties and responsibilities, subject to existing company rules and regulations, I hereby knowingly and voluntarily accept:

- a. To comply with the obligations and responsibilities set in the DLSMC Privacy Manual;
- b. To adhere to the principles of transparency, legitimate purpose, and proportionality;
- c. To keep all personal data and privileged information strictly confidential;
- d. To ensure the presence of consent of the data subjects or the appropriate lawful criteria prior to processing of personal data;
- e. To put into practice appropriate physical, technical and organizational security measures
- f. To allow the DPO to be involved from the earliest stage possible in all issues relating to privacy and data protection;
- g. To grant the DPO and other authorized personnel such as but not limited to the IT Department, external auditors and others which the DPO may deem appropriate to have access to the personal data it is processing, including the processing systems;
- h. To participate in capacity-building, orientation or training programs for employees, agents, representatives, regarding privacy and security policies;
- i. To ensure and maintain the confidentiality, integrity, availability, and resilience of data processing systems and services;
- j. To uphold and respect the rights of data subjects of DLSMC as well as its own employees;
- k. To report all security incident and personal data breach to the DPO and the breach response team.

I also hereby acknowledge the delicate and confidential nature of the personal data or personal information, sensitive personal information including privileged information, correspondingly being a data controller carries with a serious legal responsibility with that I hereby agree:

- (a) Not to collect, hold, process or use such data or information for any purpose other than those which are allowed under the company privacy policy in accordance with the Data Privacy Act of 2012 and its Implementing Rules and Regulations;
- (b) Not to use any PI or SPI for any purpose other than administrative, medical and human resources-related matters within DLSMC and/or as stated in the existing company privacy policy;
- (c) Not to disclose any PI or SPI to any third-party service provider/supplier without a Non-Disclosure Agreement (NDA) and Data Sharing Agreement.

As an employee/affiliate of DLSMC, it is my responsibility to familiarize myself with the Privacy Policy of DLSMC. I understand that the provisions stated above shall apply even after the termination or expiration of my employment or any agreement I have with DLSMC. Furthermore, I agree to conduct my duties and responsibilities in conformity with these policies and understand that breaching these standards may result in disciplinary action up to and including termination or other legal remedy available to the organization.

Signed this ____day of _____, 2020 at Delos Santos Medical Center, Quezon City, Metro Manila.

Signature over Printed Name

Position/Department

Witness



DATA PRIVACY REQUEST FORM

Important: Proof of Identity must accompany this Request Form and in proper cases, letter of authorization signed by the ward or absentee if there’s any.

Full Name*	Date requested*
Address	
Contact number *	Email address*

Put ☐☐ on the box which applies to you:

Customer/Client <input type="checkbox"/>	Employee <input type="checkbox"/>	Former Employee <input type="checkbox"/>	Intern <input type="checkbox"/>	Business Partner <input type="checkbox"/>
Supplier <input type="checkbox"/>	Job Applicant <input type="checkbox"/>	Representative/Guardian <input type="checkbox"/>	Other/s <input type="checkbox"/> Please specify: _____	

Type of Query

- ☐ Access to personal data
- ☐ Update or correction of personal data
- ☐ Request export of personal data
- ☐ Restrict or object to the use of personal data
- ☐ Delete personal data
- ☐ Question about Privacy Management Program
- ☐ Withdraw consent in processing personal data

Please specify request here:

I hereby agree that Delos Santos Medical Center can use my data for the purpose of dealing with my request, in accordance with the Data Privacy Policy of Delos Santos Medical Center, I understand that Delos Santos Medical Center may require me to verify/validate my identity before fulfilling the request.

Data Subject
Action Taken:

Date Accomplished: _____
Name and Signature of processor: _____

Should you have questions or concerns regarding this, you may contact our Data Protection Officer via email at privacy@dlsmc.ph or you may call us at +63 889-DLSMC (35762) ext. 8828.



RECORDS DISPOSAL FORM

Instructions:

- 1. Use this form to document records that have met or exceeded their retention period as defined by the Data Privacy Manual and Information Classification Policy.
- 2. If additional pages are required, records destruction form must be numbered
- 3. Category of Record pertains to whether it is Public, Internal, Confidential or Restricted as determined in the Information Classification Policy
- 4. Description of Records pertains to whether it is Electronic-Based or Paper-Based
- 5. Destruction Method pertains as to whether it is a system deletion or shredding
- 6. Once completed, have the form signed by the process owner or records manager (or more senior officer) in your department prior to disposing of the relevant records. The department must permanently retain copies of completed and signed forms.
- 7. If you have any questions about this form, please contact our Data Protection Officer.

Category of Record	Description of Records	Date Range From dd/mm/yy	Date Range To dd/mm/yy	Retention Period as per the Records Retention Schedule	Records contain *Personal Information? (Y/N)	Destruction Method
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						
10.						

Name of Approving Officer: _____

Signature: _____

Records Disposed by (employee name): _____

Signature: _____

Date Disposed: _____



De Los Santos


Medical Center

A METRO PACIFIC HOSPITAL

BPC-FORM-19-015-00

PERSONAL DATA BREACH REPORT FORM

Personal Data Breach Report Form		
Personal Information of Reporting Incident		
Full Name		
Department		
Designation		
Incident Information		
Date of Incident Reporting		
Date Incident was Discovered		
Place of Incident		
Incident Type	<div>Confirmed Breach<input type="checkbox"/></div> <div>Suspected Breach<input type="checkbox"/></div>	
#	Incident Type	
1	Loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, Flash Drive, External hard drives, iPad/tablet device, or paper record)	<input type="checkbox"/>
2	Equipment theft or failure (e.g. database, application sever failures, software/system etc.)	<input type="checkbox"/>
3	Unauthorized use of, access to or modification of data or information systems	<input type="checkbox"/>
4	Attempts (failed or successful) to gain unauthorized access to information or IT system(s)	<input type="checkbox"/>
5	Unauthorized disclosure of sensitive / confidential data	<input type="checkbox"/>
6	Hacking attack	<input type="checkbox"/>
7	Unforeseen circumstances such as a fire ,flood , earthquake etc.	<input type="checkbox"/>
8	Other	<input type="checkbox"/>
Security Incident Initial Assessment		
1. Nature of Breach	<div><div><input type="checkbox"/> Confidentiality Breach</div><div><input type="checkbox"/> Integrity Breach</div><div><input type="checkbox"/> Availability Breach</div></div>	
2. Approximate no. of data subjects or records involved	<div><div><div><input type="checkbox"/> 1~49</div><div><input type="checkbox"/> 50~100</div><div><input type="checkbox"/> 101 and above</div></div><div>Is there a minor involve? Y/N : _____</div></div>	



De Los Santos

Medical Center

A METRO PACIFIC HOSPITAL

BPC-FORM-19-015-00

3. Data Possibly involved	Description of Personal Data Involved		
	<input type="checkbox"/> Personal Information	<input type="checkbox"/> Sensitive Personal Information	<input type="checkbox"/> Other Information
*pls. provide description			
4. Remedial Actions Taken	a. Description of Measures Taken to Address the Breach		
	b. Actions taken to secure or recover personal data		
	c. Actions performed or proposed to mitigate possible harm		
	d. Actions taken to inform the data subjects *state reason of delay if any		
Employee's Confirmation			
I hereby declare that the details furnished above are true and correct to the best of my knowledge and belief.			
Full Name:		Signature	Date
Data Protection Officer Confirmation			
Full Name: Karl Marxouz R. Reyes		Signature	Date

WEBSITE DATA PRIVACY NOTICE

De Los Santos Medical Center Privacy Notice

De Los Santos Medical Center (“DLSMC”) is committed to uphold the safety and confidentiality of the Personal Information of all our data subjects. This Privacy Notice (“Notice”) therefore seeks to inform you of our policies regarding the collection, use, disclosure, retention, sharing and destruction of Personal Information of our customers and clients, as well as from our own personnel.

DLSMC has developed this Notice to ensure that all appropriate standards for Personal Information protection are in place in compliance with Republic Act No. 10173 or the Data Privacy Act of 2012 (“DPA”), its Implementing Rules and Regulations, and other applicable and related laws and regulations, including issuances and advisories of the National Privacy Commission.

What is Personal Information?

Under the DPA, Personal Information are information whether recorded in a material form or not, from which your identity is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information, would directly identify you as an individual.

Personal Information also includes Sensitive Personal Information. You may refer to the link for the list of Sensitive Personal Information as enumerated under the Data Privacy Act of 2012 <https://www.privacy.gov.ph/data-privacy-act/#13>.

Why We Collect It

We collect your Personal Information, primarily, to provide medical services to patients or to process applicant/ employee data for employment purpose. With your consent we also disclose, share or provide such data to our clients, affiliates, partners and service providers who aid us in providing you with timely and efficient services.

We may also use your Personal Information, secondarily, in cases enumerated in the consent form you will sign upon availing DLSMC services or in case of applicants during the application process.

As a data subject you have the right to withdraw your consent (subject to the applicable laws) to the processing of your Personal Information at any time by contacting us in writing.

How and When We Collect Your Personal Information

Your Personal Information may be obtained in various ways including through interviews, from application forms or correspondences, by telephone or e-mail, via our website at <http://delossantosmed.ph>, and from third party providers. Nevertheless, the

Personal Information we have are those that you have given us yourself or that of your authorized representative.

Your Personal Information is collected when:

- a. you avail of, or apply for, our services by filling out application forms or other information forms through any of our available channels (e.g. online, during admission, or through our medical personnel and representatives);
- b. you provide personal information to your doctor/s who may have referred you to DLSMC for diagnosis and treatment, whether as an in-patient or out-patient;
- c. you get in touch with us to inquire about something, file a complaint, or request for a service;
- d. you take part in our research and surveys;
- e. you participate in various activities sponsored by us or any other organization acting on our behalf, such as symposia, conferences, focus group discussions, promotional events and the like;
- f. you apply for an internship program or medical training with us to fulfill your academic and clinical requirements; and
- g. you apply for a job with us.

Use and Processing of Personal Information

The following categories generally describe the ways by which DLSMC processes your Personal Information. While this is not intended to be a very specific and detailed listing of each process per category, all the ways by which we process your Personal Information fall under one of these categories:

- a. **Your diagnosis and treatment:** we use your Personal Information, particularly your medical background and information to allow us to appropriately provide medical care and services, including diagnostics and treatment. DLSMC will disclose your Personal Information to our physicians and healthcare providers, our affiliates, subsidiaries, related entities and authorized partners (including third party providers) as part of our regular business operations for these purposes.
- b. **For benefits, payments and claims:** We may process your Personal Information for purposes of billing and payment for medical and other related services rendered. Bills may be collected from you, your insurance company, Philippine Health Insurance Corporation, your company or any third party provider. For this purpose, we may have to disclose the nature and type of your treatment and other related information that will be required for the settlement of your account.
- c. **For our business operations:** Your Personal Information will be processed as part of DLSMC's operations. This includes our general business management operations, quality control and assessment, employee and/or staff evaluation and financial performance reporting.
- d. **Performance of a legal obligation:** Under the law, DLSMC is required to share your Personal Information to government authorities in certain instances. This may occur for instance when DLSMC may be required to provide documentary and/or testimonial

evidence in court proceedings that may require the disclosure of your Personal Information. We may also be required to provide sensitive personal information or health information in compliance with RA 11332 or Law on Reporting of Communicable Diseases to proper government authorities.

e. **Marketing and other legitimate commercial purposes.** We may also use your Personal Information to contact you with newsletters, information campaigns, marketing or promotional materials and other information that may be related to the services we provide, and also to further improve the quality of our services.

Other uses and disclosures of your Personal Information

Outside of the purposes stated above, other uses and disclosures of your Personal Information will only be made:

- a. with your express consent,
- b. in case of an emergency, or
- c. when otherwise permitted or required by law.

d. Such circumstances where disclosure of your Personal Information is pursuant to an order of a court or tribunal, or when such disclosure is required under existing laws and regulations.

In like manner, we may use and disclose your Personal Information to:

- a. your visitors when they wish to inquire about you in the patient directory, and
- b. other people involved in, or interested in your healthcare, such as your family members, loved ones or any other person you identify as being involved in your healthcare. In case you are not capable of agreeing or objecting to such disclosure, we will use our judgment in determining whether the use or disclosure is in your best interest.

In these cases, we ensure that your Personal Information is disclosed on a confidential basis, and is always subject to the applicable Privacy Laws. We will never share or sell your personal information to third party providers not affiliated with DLSMC except in circumstances determined in our Data Privacy Policy

Who has access to your Personal Information?

The following will have access to your Personal Information:

- a. Healthcare professionals including but not limited to members of DLSMC's medical staff, nurses and other healthcare providers, either pursuant to an employment contract or any other arrangement. They will have access to your Personal Information because they are authorized to enter information into your medical records, as well as to review or update the same.
- b. All departments and units in DLSMC who will need your personal information in the performance of their functions. For example, certain treatments or procedures require that your Personal Information be shared across different departments of DLSMC.
- c. Any member of a volunteer, religious or charitable/non-profit organization who is allowed to provide assistance within DLSMC. This includes priests, pastors or heads of other religious organizations who provide religious rites to patients or the deceased.
- d. All of our non-medical employees, staff or personnel who may need access to your information in the performance of their duties. For example, our employees will access your Personal Information in order to prepare your

billing statement. Likewise, your medical information will be needed for your dietary needs during your confinement.

- e. All entities operating within the premises of DLSCMC, including, but not limited to housekeeping and security. DLSCMC may share your personal information with these entities for the purposes stated above.

How do we secure and protect your Personal Data?

Our Privacy Notice applies to your Personal Information that we have collected. DLSCMC creates and maintains a record of your Personal Information in its offices to serve you better. Under the DPA, DLSCMC is likewise required to protect your Personal Information, and to process such data only in accordance with the following data privacy principles:

a. Transparency: We are obligated to inform you of the nature, purpose and extent of why we are processing of your Personal Information, including the risks and safeguards involved, the identity of the persons involved in the processing of your personal data, your rights as data subject, and how these rights can be exercised.

b. Legitimate purpose: We will only process your Personal Information for a legitimate purpose, compatible with our declared and specified purpose, and not contrary to the law, accepted morals and public policy.

c. Proportionality: We will process your Personal Information as adequate, relevant, suitable, necessary and not excessive in relation to the declared and specific purpose. Your Personal Information is stored in a manner that reasonably protects it from misuse and loss, and from unauthorized access, modification or disclosure. We strictly enforce our Privacy Policy and have put in place technical, organizational and physical security measures that are designed to protect your Personal Information from unauthorized access, use, alteration, and disclosure.

When your Personal Information is no longer needed for the purpose for which it was obtained, we will take reasonable steps to dispose or permanently anonymize the said data. However, most of the personal information is or will be stored in files that will be kept by us for the minimum period provided under existing laws and regulations.

How can I access my Personal Data?

You may gain access to the Personal Data that we have lawfully collected from you in order to update and/or correct it, subject to certain exceptions. If you wish to access your Personal Data, please contact us in writing and we will respond to you within a reasonable timeframe. Please take note that our ability to respond to your request may depend on the circumstances regarding our collection of your Personal Information.

We may charge a reasonable administrative fee for providing a copy of your Personal Data.

In order to protect your Personal Data, we may require identification from you before releasing the requested information.

On another note, we may be restricted by law or certain regulation from giving you access to a personal data without proper authorization as required by law or existing regulations.

Links to Other Websites

Our website may contain links that enable you to easily visit other websites of interest.

However, once you have clicked a link that leads you away from our site, please take note that we do not have any control over other websites. Therefore, we cannot be responsible for the protection and privacy of any information that you have provided whilst visiting such sites. Moreover, such sites are not governed by this privacy statement. Therefore, we advise you to exercise caution and read the privacy statement (if applicable) of the website/s that you are visiting.

Changes to the Privacy Notice and Privacy Policy

From time to time, we may change or update our Privacy Statement, Privacy Policy and related practices to comply with government and regulatory requirements, to adapt to new technologies and protocols, to align with industry practices, or for other legitimate purposes.

Know More

As data subjects, you are afforded certain rights in relation to your Personal Information under the Data Privacy Act of 2012. As such, we constantly ensure that we have your consent to collect, use, disclose, retain and dispose your Personal Information for the purposes that we have identified. You have the right to be informed of these specific rights, to object to the processing of your Personal Information, to access, update and correct your Personal Information, and to withdraw your consent and/or edit your consent preferences at any time.

If you wish to have access to your Personal Information from our records; believe that such Personal Information that we have of you are incomplete, not up-to-date, or inaccurate; or have any queries or complaints about our Privacy Policy, you may get in touch with the DLSCMC's Data Privacy Officer through the contact details provided below:

Address: 201 E. Rodriguez Sr. Blvd., Quezon City 1112 Philippines

Telephone: +632 889-DLSCMC (889-35762) ext. 8828

E-mail: privacy@dlsmc.ph

Your rights as data subject are provided in Section 16 of the DPA, which you may access here: <https://www.privacy.gov.ph/data-privacy-act/#16>.

You may also contact the National Privacy Commission through the following contact details:

Address: 5th Floor, East Banquet Hall, Delegation Building

Philippine International Convention Center, Pasay City, Metro Manila 1307

Phone: +632 9399638715 / +632 9451534299

E-mail: info@privacy.gov.ph

Website: <https://privacy.gov.ph>

Cookie Policy

This is the Cookie Policy for De Los Santos Medical Center, accessible from <https://delossantosmed.ph/>

What Are Cookies

Cookies are text files placed on your computer to collect standard Internet log information and visitor behavior information. These are downloaded to your computer, to improve user experience. This page describes what information DLSCMC gather, how such information is used and why DLSCMC need to store these cookies.

To allow users to exercise their right to object, DLSCMC will also share how users can prevent these cookies from being stored. However, this may downgrade or 'break' certain elements of the sites functionality. For more general information on cookies, please read "What Are Cookies".

How We Use Cookies

We use cookies for a variety of reasons detailed below. Unfortunately, in most cases there are no industry standard options for disabling cookies without completely disabling the functionality and features they add to this site. It is recommended that you leave on all cookies if you are not sure whether you need them or not in case they are used to provide a service that you use.

How to manage or disable Cookies

You can prevent the setting of cookies by adjusting the settings on your browser (see your browser Help for how to do this). Be aware that disabling cookies will affect the

functionality of this and many other websites that you visit. Disabling cookies will usually result in also disabling certain functionality and features of DLSCMC website. Therefore, it is recommended not to disable cookies.

What Cookies We Use

Login related cookies

We use cookies when you are logged in so that we can remember this fact. This prevents you from having to log in every single time you visit a new page. These cookies are typically removed or cleared when you log out to ensure that you can only access restricted features and areas when logged in. Log in related cookies are collected by using/logging in credentials to your DLSCMC My Results Account.

Email newsletters related cookies

This site offers newsletter or email subscription services and cookies may be used to remember if you are already registered and whether to show certain notifications which might only be valid to subscribed/unsubscribed users. Email newsletters related cookies when you subscribe to DLSCMC's Newsletter wherein your name, surname and email address is collected.

Third Party Cookies

In some special cases DLSMC also use cookies provided by trusted third parties. The following section details which third party cookies you might encounter through this site.

From time to time DLSMC test new features and make subtle changes to the way that the site is delivered. When DLSMC are still testing new features these cookies may be used to ensure that you receive a consistent experience whilst on the site whilst ensuring we understand which optimizations users appreciate the most.

More Information

Hopefully that has clarified things for you and as was previously mentioned if there is something that you aren't sure whether you need or not it's usually safer to leave cookies enabled in case it does interact with one of the features you use on our site.

For questions and other concerns regarding our Cookie Policy or Privacy Policy you may contact us at privacy@dlsmc.ph or call us at +632 89-DLSMC (89-35762) ext. 8828.



DATA PRIVACY NOTICE

Delos Santos Medical Center is committed to comply with the Data Privacy Act of 2012, its Implementing Rules and Regulations and NPC Orders, Issuances and Advisory.

It is our duty to respect every individual’s right to privacy as much as we aim to ensure the safety and security of everyone inside the Hospital premises.

WHAT WE COLLECT. DLSMC will only collect basic information about you by asking you to sign our official log books. The data we will collect includes your name, company, purpose of visit, destination, time of arrival and departure, signature and a video footage recorded via CCTV system inside the premises. For those with vehicles, we take note of your vehicle plate number and a video footage is also being recorded via a CCTV system installed in all hospital entry and exit points.

WHY WE COLLECT THEM. The data we collect is for the purpose of allowing us to implement appropriate security measures to protect your interest and that of Delos Santos Medical Center. It will also help us investigate reported violations of Hospital policies and other infractions of the law. Lastly, the data we collect will be used to generate statistics useful in improving hospital policies and services.

HOW WE USE, STORE, AND RETAIN THEM. Your data are kept in a place inside the Hospital where at least one security personnel is on-duty 24/7. Only authorized Hospital and security personnel have access to them. We dispose of the log books two (2) years from the date of collection, unless required by law to retain them for a longer period. CCTV footages, on the other hand, are stored for thirty (30) days before being automatically deleted. We do NOT transfer, disclose or share your personal data with other persons or organizations, unless required or permitted by law.

HOW YOU MAY EXERCISE YOUR RIGHTS. You have rights under the law regarding your personal data such as the right to access CCTV footage and images and/or request for copies. Should you wish to exercise them, or if you just happen to have some questions, you may contact the Data Protection Officer by email privacy@dlsmc.ph or call us at +63 2 8778828, or by mail to 201 E. Rodriguez Sr. Blvd, Quezon City, 1112 Philippines.



DATA SHARING AGREEMENT

This Data Sharing Agreement was made and entered into on _____ by and between:

DELOS SANTOS MEDICAL CENTER, a corporation duly organized and existing under the laws of the Republic of the Philippines, with principal place of business at 201 E Rodriguez Sr. Ave, Quezon City, 1112 Metro Manila Philippines, represented herein by its President and CEO, **Elizabeth G. Dantes** (hereinafter referred to as the “**DLSMC**”);

and

Service Provider, a corporation duly organized and existing under the laws of the Republic of the Philippines, with office address at _____, Philippines, represented herein by its Position and Designation, **SIGNATORY**, (hereinafter referred to as “Service Provider”);

WITNESSETH: That

WHEREAS, the **DLSMC** engaged the services of the **Service Provider** to provide _____ which engagement is covered by a separate agreement identified as the **NAME OF AGREEMENT** executed on _____;

WHEREAS, the parties acknowledge that pursuant to the **NAME OF AGREEMENT**, the **DLSMC** will disclose or make available Personal Data to the **Service Provider**;

WHEREAS, the parties acknowledge that pursuant to the **NAME OF AGREEMENT**, the parties have agreed to incorporate the following provisions of this Data Sharing Agreement;

WHEREAS, this Data Sharing Agreement is entered into pursuant to the Data Privacy Act of 2012 (the “Data Privacy Act”) and its Implementing Rules and Regulations (IRR), which requires a data sharing agreement prior to the collection and sharing by the **DLSMC** of Personal Data to the **Service Provider**;

NOW, THEREFORE, for and in consideration of the premises and mutual obligations contained herein, the parties hereby agree as follows:

- 1. **Purpose**
The company will share or disclose personal data for the purpose of _____
- 2. Whenever applicable, in performing the obligation of the Service Provider under this contract, the Service Provider shall, at all times, comply with the provisions of Republic Act No. 10173 or “the Data Privacy Act of 2012,” its implementing rules and regulations, and all other laws and government issuances relating to data privacy and the protection of personal data. The Service Provider, its officers, employees, agents, and representatives, shall, among others:

- a) Process the Personal Data from the COMPANY for the following purposes only: (i) Processing in accordance with the Data Sharing Agreement; and (ii) Processing to comply with other reasonable instructions given by the COMPANY where such instructions are consistent with the terms of the Data Sharing Agreement.
- b) Refrain from making use of the personal data for any purpose other than as specified by **DLSMC**. The Service Provider will inform the COMPANY of any such purposes which are not contemplated in this Data Sharing Agreement.
- c) Not to sub-contract or engage a third party to process the Personal Data shared/disclosed by **DLSMC** without the prior knowledge and written agreement of the **DLSMC**, and only after the third party has provided all the necessary assurance and guarantees that it has adequate security measures to protect the Personal Data.
- d) Process personal data only upon the documented instructions of the **DLSMC**, including transfers of personal data to another Personal Information Controller or Processor, unless such transfer is authorized by law;
- e) Maintain proper records, and provide the **DLSMC** access to such records, as will allow the **DLSMC** to comply with the exercise by data subjects of their rights under the Data Privacy Act of 2012;
- f) Determine appropriate level of security measures, subject to, and in conjunction with, that of the **DLSMC**, taking into account the nature of the personal information to be protected, the risks represented by the processing, the size of the organization and complexity of its operations, current data privacy best practices, and cost of security implementation;
- g) Implement reasonable and appropriate organizational, physical, and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration, and disclosure, as well as against any other unlawful processing, or for such other purposes as may be required under the Data Privacy Act of 2012 or any other applicable law or regulation;
- h) Ensure that its employees, agents, and representatives who are involved in the processing of personal information operate and hold personal information under strict confidentiality. This obligation shall continue even after their transfer to another position or upon termination of their employment or contractual relations;
- i) In case of data breach, as when sensitive personal information that may, under the following circumstances, be used to enable identity fraud; or are reasonably believed to have been acquired by an unauthorized person; the **DLSMC**, Service Provider or the National Privacy Commission believes that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject, the Service Provider shall promptly notify the **DLSMC** within twenty-four (24) hours or earlier upon knowledge or when there's a reasonable belief that a personal data breach occur, to enable the **DLSMC** to notify the National Privacy Commission and the affected data subject within the period prescribed under the Data Privacy Act of 2012,
- j) Make available to the **DLSMC** all information necessary to demonstrate compliance with the obligations laid down in the Data Privacy Act of 2012, and allow for and contribute to audits, including inspections, conducted by the **DLSMC** or another auditor mandated by the latter; and
- k) Include all the foregoing in the privacy and security policy of the PROVIDER.

3. Additional requirements by Delos Santos Medical Center

- a. Destruction and Return of Personal Data
 - i. In order to protect Personal Data, the **Service Provider** shall store and process Personal Data securely, and destroy it confidentially when it is no longer necessary in accordance with the **DLSMC**'s instructions.
 - ii. Personal Data in the custody of the **Service Provider** that requires disposal shall be disposed or discarded by the **Service Provider** in a secure manner that would prevent further processing, unauthorized access or disclosure to any other party.
- b. Upon request by the **DLSMC**, the **Service Provider** shall allow the **DLSMC** or its representatives to audit the Service Provider's premises, systems, procedures, documents and personnel as may be desirable or necessary to ensure compliance with this Data Sharing Agreement and/or with the Data Privacy Act and its Implementing Rules and Regulations.
- c. This Data Sharing Agreement shall prevail over the confidentiality, disclosure and data management provisions of the **NAME OF AGREEMENT** only in case of conflict or inconsistency.
- d. Without prejudice to its liability for breach of any of its obligations under the **NAME OF AGREEMENT**, the **Service Provider** shall indemnify **DLSMC** in full for costs, losses, charges or expenses it suffers arising out of any Personal Data Breach whether due to the negligence or otherwise on the part of the **Service Provider**.

4. Miscellaneous

- a. Severability – If any provision in this Data Sharing Agreement or any document or instrument relevant, executed or delivered pursuant hereto shall be held invalid, the remainder thereof shall not be affected thereby.
- b. Amendment - This Data Sharing Agreement and the terms and conditions hereof may not be changed, discharged, amended, modified or altered unless in writing and duly signed by an authorized representative of each of the parties.
- c. Indemnity - The **Service Provider** agrees to indemnify and hold the **DLSMC**, its officers, employees and personnel harmless from any damages, loss, liability or costs (including reasonable attorneys' fees and the costs of enforcing this indemnity) arising out of or resulting from any breach of the **Service Provider**'s obligation under or in connection with this Data Sharing Agreement, including any breach of applicable mandatory statutory obligations.

The parties agree that any Data Subject, who has suffered damage as a result of any breach by **Service Provider** of its obligations in this Data Sharing Agreement is entitled to receive compensation from the **Service Provider** for the damage suffered.

- d. Remedies - The rights or remedies of the **DLSMC** under this Data Sharing Agreement shall not be deemed to be the exclusive remedies for a breach of this Data Sharing Agreement, but shall be in addition to any other rights or remedies at law, in equity or otherwise available to the **DLSMC**.

No failure on the part of the **DLSMC** to exercise, and no delay in exercising, any right or remedy under or in connection with this Data Sharing Agreement shall operate as a waiver thereof. No single or partial exercise of any right or remedy under or in connection with this Data Sharing Agreement preclude any other or a future exercise thereof or the exercise of any other right or remedy, whether of a similar or dissimilar nature, Delos Santos Medical Center may have by virtue of this Data Sharing Agreement.

- e. Assignment - This Data Sharing Agreement shall be binding upon and be enforceable against the parties hereto and their respective successors and assigns, except that the **Service Provider** shall not be allowed to assign, transfer or convey any of his rights, privileges, interest or obligations under this Data Sharing Agreement without the prior written consent of _____ the **DLSMC**.
- f. Governing Law & Venue of Action - This Data Sharing Agreement shall be governed by _____ and construed in accordance with the Philippine laws. Any legal action, suit or proceeding arising out of or relating to this Data Sharing Agreement shall be instituted exclusively in the _____ City _____ Court _____ of _____ Quezon _____ City.
- g. The obligations and liabilities of the **Service Provider** arising from this Data Sharing Agreement shall survive the termination or expiration of the **NAME OF AGREEMENT**.
- h. All personal data processed on behalf of the **DLSMC** shall remain the property of the **DLSMC** _____ and/or _____ the _____ relevant _____ Data _____ subjects.
- i. Effectivity - This Data Sharing Agreement shall take effect immediately upon its execution and shall continue to be in effect until a new agreement takes place, which may be renewed on the ground that the purpose or purposes of such agreement continues to exist.

IN WITNESS WHEREOF, the parties hereto have set their hand this _____, 2019 in, Quezon City, Philippines.

Delos Santos Medical Center

Company Name

Elizabeth G. Dantes
President & CEO

Authorized Signatory
Designation/ Position

Witnesses:

ACKNOWLEDGEMENT

REPUBLIC OF THE PHILIPPINES)
_____) S.S.

BEFORE ME, a duly authorized notary public for and in the above-named jurisdiction, personally appeared on this _____, 20__, the following, who are personally known to me and/or identified through competent evidence of identity, to wit:

Name	Competent Evidence of Identity (Type of I.D./I.D. No.)	Issued on/at and/or Valid until
------	--	---------------------------------

known to me and to me known to be the same persons who executed the foregoing instrument, and who acknowledged before me that their respective signatures on the instrument were voluntarily affixed by them for the purposes stated therein, and who declared to me that the said instrument is their free and voluntary act and deed and that of the partnership/entity represented, and are duly authorized to sign, if acting in a representative capacity.

I further certify that this instrument refers to a Data Sharing Agreement, consisting of _____ (__) pages, including this page wherein the acknowledgment is written and has been signed by the herein parties and their witnesses.

IN WITNESS WHEREOF, I hereunto set my hand and affix my notarial seal on the date and at the place above written.

Notary Public

Doc. No.

Page No.

Book No.

Series of 2020.



DATA PRIVACY COMPLAINTS AND INQUIRIES PROCEDURE

I. Introduction

- a. De Los Santos Medical Center (DLSMC) is committed to maintaining the privacy of individual's personal information at all times to ensure compliance with the Data Privacy Act of 2012 and other issuances and advisories of the National Privacy Commission.
- b. DLSMC undertakes several transactions internally and externally with the general public which involve the processing of personal information. These transactions are conducted through phone, letters, emails, online and face to face contact. DLSMC recognizes that in this environment, errors, misunderstandings and unexpected problems can occur. Consequently, DLSMC is committed in providing an effective, efficient and responsive data privacy complaints handling process, which promotes transparency and openness.

II. OBJECTIVES

- a. This document sets out the procedures that DLSMC will follow in the event that a data privacy inquiry or data privacy complaint is received.
- b. These procedures are not intended to apply to requests for access to, or correction of, personal data. This document is to guide DLSMC in dealing with the exercise the data subject's right to file a complaint.

III. SCOPE

- a. This procedure covers inquiries or complaints raised to DLSMC that relates to data privacy. This procedure should be read in conjunction with the Data Privacy Manual.

IV. DEFINITION OF TERMS

- a. **Data Privacy Act of 2012** is an act protecting individual personal information in Information and Communications Systems in the Government and the Private Sector, creating for this purpose a National Privacy Commission, and for other purposes.
- b. **Data Protection Officer** is the person designated by DLSMC whose primary function is to monitor and oversee the company's compliance with the Data Privacy Act, its Implementing Rules and Regulations and related issuances.
- c. **Disclosure** is the act or process of revealing or uncovering a material fact or an item of information.
- d. **Personal Data Breach** refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed. A personal data breach may be in the nature of:
 4. An availability breach resulting from loss, accidental or unlawful destruction of personal data;
 5. Integrity breach resulting from alteration of personal data; and/or
 6. A confidentiality breach resulting from the unauthorized disclosure of or access to personal data
- e. **Personal Information** refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.

- f. **Privacy complaint** is a complaint made by or on behalf of an individual about an act or practice of DLSMC in relation to the individual's personal information that is in violation of DLSMC's obligations under the Data Privacy Act of 2012.

V. SCOPE AND LIMITATIONS

This policy shall apply to all privacy complaints brought upon by data subjects of DLSMC with the exception of personnel employed by a third-party service provider.

This shall be limited only to privacy concerns involving personal data processed by DLSMC and shall not in any manner extend to complaints brought upon by data subjects where DLSMC is not a party thereto.

This procedure shall be read in conjunction with all other existing policies of Delos Santos Medical Center, the existing provisions of RA 10173 and relevant issuances of the National Privacy Commission

VI. PROCEDURE

- a. Should any data subject have inquiries relating to the Data Privacy Policy, DLSMC employees should refer them to DLSMC's Data Privacy Officer:
 - i. Email Address: privacy@dlsmc.ph
 - ii. Telephone Number: +63 889-DLSMC (35762) ext. 8828; +63 877 8828
 - iii. Mobile Number: +63 9357004157
- 2 In the event that a data privacy complaint is received by DLSMC, the following procedures will apply:
 - 2.1 If a verbal data privacy complaint is received via phone, DLSMC personnel should encourage the complainant to submit their complaint in writing to the DLSMC's Data Privacy Officer using the DLSMC's Data Privacy Complaint Form. If the complainant is unwilling to submit a written complaint, then the DLSMC personnel receiving the complaint should:
 - a. Document the verbal complaint in writing.
 - b. Capture the complainant's contact details for the purposes of contacting them in relation to their data privacy complaint. At a minimum, this should include the complainant's telephone number, but ideally would also include an email or postal address.
 - c. Advise the complainant that details of the data privacy complaint and their contact details will be forwarded to DLSMC's Data Privacy Officer for the purposes of assessing, investigating, conciliating and reporting on the data privacy complaint.
 - d. If the complainant is unwilling to provide their contact details, advise the complainant that it may be difficult to properly investigate or respond to their complaint and it will not be possible for DLSMC to provide response to the complainant.
 - e. Refer the data privacy complaint to the DLSMC's Data Privacy Officer within 24 hours.
 - 2.2 If a written data privacy complaint is received, the DLSMC personnel should within 24 hours forward the complaint to DLSMC's Data Privacy Officer.

The Data Privacy Officer will undertake the following:

- a. Acknowledge the individual's data privacy complaint within 5 business days of the complaint having been received.
- b. Liaise with the complainant as appropriate to seek any relevant information necessary to investigate the data privacy complaint.
- c. Impartially assess and investigate the data privacy complaint in consultation with the relevant DLSMC department.
 - i. The root cause of the breach or reported violation or incident must be established
 - ii. Action should be taken to mitigate damage or prevent

- d. Appropriately document the investigation process.
- e. Advise the complainant of the outcome of the investigation and the proposed action, if any, DLSCM intends to take.
 - Provide the complainant with information on how to make a complaint to the National Privacy Commission if they are unhappy with the outcome of DLSCM's investigation.
 - National Privacy Commission
 - 5th Floor, Delegation Building, PICC Complex, Roxas Boulevard, Pasay City, Metro Manila
 - Phone: (02) 8234 2228
 - Email: complaints@privacy.gov.ph
- f. If the outcome of the investigation concludes that DLSCM appears to have mishandled an individual's personal information, the DPO must liaise with the relevant DLSCM department over what steps are appropriate to take to ensure similar incident does not occur again.
 - i. Policies and procedures should be updated to prevent recurrence
 - ii. Capacity Building for all employees.
 - iii. Accomplish reportorial requirements by the National Privacy Commission with respect to security incidents.
- g. If what transpired is a security incident or a personal data breach, the DPO shall commence the Security Incident Response Policy and Procedure.
- h. The DPO shall conduct the investigation and seek assistance with the HR department for imposition of penalties as well as determination of appropriate disciplinary action against the involved employee.

VII. **Annex**

- a. Data Privacy Complaint Form

DATA PRIVACY COMPLAINT FORM

An asterisk (*) denotes mandatory items. Not replying to mandatory items in the form would leave us unable to properly investigate the complaint and may render your complaint inadmissible.

Full Name*	Contact No. *	Date filed*
Address	Email address*	

Put ✓ on the box which applies to you:

* Are you

☐ (a) personally affected by the issue(s) at stake in your complaint.

☐ (b) not personally concerned, but would like to draw the attention of DPO to an alleged violation of DLSMC Data Privacy Policy and Procedure.

Customer/Client <input type="checkbox"/>	Employee <input type="checkbox"/>	Former Employee <input type="checkbox"/>	Intern <input type="checkbox"/>	Business Partner <input type="checkbox"/>
Supplier <input type="checkbox"/>	Job Applicant <input type="checkbox"/>	Representative/Guardian <input type="checkbox"/>	Other/s <input type="checkbox"/> Please specify: _____	

Please describe your complaint and specify which policy, privacy law or right you believe have been infringed by DLSMC, its employee and/or its affiliates. (Please be as specific as possible with dates, times and the specific policy, procedure or action taken; include the names, if any, of any one in DLSMC with whom you discussed this. Use the other side of this form if you need more room.)

Date &Signature:* _____

Please explain what you would like the institution to do in order to remedy the alleged breach(es) or infringements.

De Los Santos Medical Center treats all complaints confidentially. However, the investigation of your complaint may require disclosing your identity and the allegations you made to DLSMC, its employees and/or its affiliates against which you complained and, if necessary for the investigation, to the third parties involved, including the National Privacy Commission, where relevant.

For questions and data privacy concerns, you may contact our Data Protection Officer via email at privacy@dlsmc.ph or you may call us at +63 889-DLSMC (35762) ext. 8828. You can visit our privacy statement here <https://www.delossantosmed.ph/privacy-policy>.



SECURITY INCIDENT RESPONSE POLICY AND PROCEDURE

I. Introduction

General information

This policy and procedure was developed for Delos Santos Medical Center (hereafter referred to as “DLSMC”) and classified as its confidential property. Due to the sensitive nature of the information contained herein, this manual is available only to members of the data breach response team, and those who otherwise play a direct role in security incident management and data breach management.

Unless otherwise instructed, each plan recipient will receive and maintain two copies of the plan, stored as follows:

Unless otherwise instructed, each plan recipient will receive and maintain two copies of the plan, stored as follows:

- One copy in recipient's office
- One copy in recipient's home

The security incident response policy and procedure and personal data breach management effort of DSLMC recognizes and affirms the importance of data subjects, personal data, processes, and technology of DSLMC.

It is the responsibility of each manager, process owner and employee to safeguard and keep confidential all personal data and corporate assets contained herein.

II. Overview and objectives

This security incident management policy and personal data breach management establishes the recommended organization, actions, and procedures needed to

- Manage security incidents, including personal data breach.
- Create a data breach response team;
- Implement organizational, physical and technical security measures and personal data privacy policies;
- Implement an incident response procedure;
- Mitigate possible harm and negative consequences of security incident and/or data breach;
- Comply with the Data Privacy Act of 2012, its IRR, and all related issuances;
- Support the business recovery efforts in restoring the integrity, availability and confidentiality of personal data in the aftermath of the security incident and/or data breach.

The security incident management policy and personal data breach management should conform to the Privacy Policy and Privacy Management Program of **DLSMC**.

III. Scope

This security incident management policy includes initial actions and procedures to respond to events that tends to affect data protection, or may compromise the confidentiality, availability and integrity of personal data. It includes incidents that may result in a personal data breach, if not for safeguards that have been put in place and those that have a critical impact on the business activities of **DLSMC**.

The **DLSMC** Security Incident Management Plan is designed to provide an initial response to any security incident and data breach, such as unlawful destruction, loss or alteration of personal data, including unauthorized disclosure or an event or situation that affects or will likely affect data protection or compromise the availability, integrity and confidentiality of personal data. This document defines the requirements, strategies and proposed actions needed to respond to such eventualities.

Exclusions

This plan specifically excludes the following from its scope:

- Facilities, establishments or offices of personal information processor, clients and third-party service providers.

IV. Security Incident Management Plan

A. Creation of Security Incident and Breach Management Team

Security Incident Management Team comprising of six (8) officers shall be responsible for ensuring immediate action in the event of a security incident or personal data breach. The team shall conduct an initial assessment of the incident or breach in order to ascertain the nature and extent thereof. It shall also execute measures to mitigate the adverse effects of the incident or breach.

The team shall be divided into three groups who shall have their respective duties namely:

a) Threat Assessment Group

The Threat Assessment Group shall be composed of the CIO or the IT head, the AVP for Engineering and the AVP for Nursing Services. They shall be responsible in securing and restoring the personal data that were compromised and should be able to restore the confidentiality, integrity and availability of the same.

b) Damage Assessment Group

The Damage Assessment Group shall be composed of the Corporate Communication Manager and the Medical Records Section Head. They shall be responsible in proposing and performing acts to mitigate possible harm or negative consequences and limit the damage or distress to those data subjects affected by the incident.

c) Breach/Incident Management Group

The Breach/Incident Management Group shall be composed of the AVP for HR and the Business Process and Compliance Head. They shall be responsible in making sure that the security incident management policy is being implemented accordingly. They shall see to it that notifications were made as to the affected data subjects as well as to the National Privacy Commission and all

other functions required by the Data Privacy Act of 2012, its relevant provisions, its IRR and all related issuances of the Commission on personal data breach management.

The Data Protection Officer shall be involved in all stages of the security incident which is from Threat Assessment to Breach/Incident Management. He must coordinate and report to the head of the organization, the National Privacy Commission with regard to commission issued orders and compliance orders and in proper cases, to other local authorities such as but not limited to the NBI, PNP and DICT.

B. The Security Incident Response Team is responsible for:

- a) **Implementing security incident management policy** of the personal information controller or personal information processor;
- b) **Managing security incidents** and personal data breaches; and
- c) **Compliance** by the personal information controller or personal information processor with the relevant provisions of the Act, its IRR, and all related issuances by the Commission on personal data breach management.

The members must, as a collective unit, be ready to:

- a. Assess and evaluate a security incident;
- b. Restore integrity to the information and communications system;
- c. Mitigate and remedy any resulting damage, and comply with reporting requirements.

C. Composition

The Data Breach Response Team shall be composed of the following members who shall directly report to the Data Protection Officer regarding data breach and security incident involving personal data.

Name	Job	Department	Contact No.	Email Address
1. Madeline J. Carls	AVP	Human Resources	Primary: 8935762 loc 3807	Primary: mjcarls@dlsmc.ph
2. Ryan M. Empleo	Quality Management and Patient Safety	Medical Affairs	Primary: 8935762 loc 3365	Primary: rmempleo@dlsmc.ph
3. Ofelia E. Hernando	Senior AVP	Hospital Operations	Primary: 8935762 loc 3810	Primary: oehernando@dlsmc.ph
4. Engr. Deidre Malapitan	AVP	Engineering and Maintenance	Primary: 8935762 loc 3806	Primary: damalapitan@dlsmc.ph
5. Charito T. Perez	Medical Records Senior Manager	Medical Affairs	Primary: 8935762 loc 3628	Primary: ctperez@dlsmc.ph
6. Randy S. Sac	Chief Information Officer	Information Technology	Primary: 8935762 loc 3897	Primary: rssac@dlsmc.ph

7. Jake Christian T. Solomon	Marketing Manager	Marketing	Primary: 8935762 loc 3192	Primary: jtsolomon@dlsmc.ph
8. Karl Marxcuz R. Reyes	DPO	Business Process and Compliance	Primary: 09357004157 / 8935762 loc 8828	Primary: krreyes@dlsmc.ph
9. Frederick Charles G. Rodriguez	Department Head	Business Process and Compliance	Primary: 8935762 loc 3808	Primary: fgrodriguez@dlsmc.ph

D. Implementation of Security Measures

The company shall implement reasonable and appropriate physical, technical and organizational measures for the protection of personal data. These security measures aims to maintain the availability, integrity and confidentiality of personal data and protect them against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination.

A. Organization Security Measures

a. Data Protection Officer (DPO)

The designated DPO is **Mr. Karl Marxcuz R. Reyes** from Business Process and Compliance Department.

b. Functions of the DPO and/or any other responsible personnel with similar functions.

The DPO shall oversee the compliance of the organization with the DPA, its IRR, and other related policies, including the conduct of a Privacy Impact Assessment, implementation of security measures, security incident and data breach protocol, and the inquiry and complaints procedure.

Duties and Responsibilities of the DPO:

- a. Monitor the PIC’s or PIP’s compliance with the DPA, its IRR, issuances by the NPC and other applicable laws and policies. For this purpose, he or she may:
- 1. collect information to identify the processing operations, activities, measures, projects, programs, or systems of the PIC or PIP, and maintain a record thereof;
 - 2. analyze and check the compliance of processing activities, including the issuance of security clearances to and compliance by third-party service providers;
 - 3. inform, advise, and issue recommendations to the PIC or PIP;
 - 4. ascertain renewal of accreditations or certifications necessary to maintain the required standards in personal data processing; and
 - 5. advice the PIC or PIP as regards the necessity of executing a Data Sharing Agreement with third parties, and ensure its compliance with the law;

- b. Ensure the conduct of Privacy Impact Assessments relative to activities, measures, projects, programs, or systems of the PIC or PIP;
- c. Advise the PIC or PIP regarding complaints and/or the exercise by data subjects of their rights (e.g., requests for information, clarifications, rectification or deletion of personal data);
- d. Ensure proper data breach and security incident management by the PIC or PIP, including the latter's preparation and submission to the NPC of reports and other documentation concerning security incidents or data breaches within the prescribed period;
- e. Inform and cultivate awareness on privacy and data protection within the organization of the PIC or PIP, including all relevant laws, rules and regulations and issuances of the NPC;
- f. advocate for the development, review and/or revision of policies, guidelines, projects and/or programs of the PIC or PIP relating to privacy and data protection, by adopting a privacy by design approach;
- g. Serve as the contact person of the PIC or PIP vis-à-vis data subjects, the NPC and other authorities in all matters concerning data privacy or security issues or concerns and the PIC or PIP;
- h. Cooperate, coordinate and seek advice of the NPC regarding matters concerning data privacy and security; and
- i. Perform other duties and tasks that may be assigned by the PIC or PIP that will further the interest of data privacy and security and uphold the rights of the data subjects.

Duties and Responsibilities of the Business Process and Compliance Department:

Except for items (a) to (c), the BPC shall perform all other functions of a DPO. Where appropriate, BPC shall also assist the DPO in the performance of the latter's function.

- a. Conduct of trainings or seminars to keep personnel, especially the Data Protection Officer updated vis-à-vis developments in data privacy and security

The organization shall sponsor a mandatory training on data privacy and security at least once a year. For personnel directly involved in the processing of personal data, management shall ensure their attendance and participation in relevant trainings and orientations, as often as necessary.

- b. Conduct of Privacy Impact Assessment (PIA)

The organization shall conduct a Privacy Impact Assessment (PIA) relative to all activities, projects and systems involving the processing of personal data. It may choose to outsource the conduct a PIA to a third party. PIA shall be conducted annually to be supervised and facilitated by the DPO to assess, evaluate and manage new risks, should there be, presented by the processing activities.

- c. Recording and documentation of activities carried out by the DPO, or the organization itself, to ensure compliance with the DPA, its IRR and other relevant policies.

The company, through the DPO with the assistance of the team, shall maintain a detailed and accurate documentation of all activities, projects and processing activities carried out in compliance with the requirements of the DPA, its IRR and issuances of the NPC.

d. Registration of data Processing System

The organization shall, through its DPO, register its data processing systems with the NPC in accordance with NPC Circular 17-01 and other relevant regulations.

e. Duty of Confidentiality

Employees, agents or representatives of the organization shall hold and operate personal data under strict confidentiality. Confidentiality shall continue even upon termination of employment/engagement contract.

Employees, who are process owners, shall be asked to sign a Confidentiality Agreement to maintain the confidentiality of personal data they are processing while employed in the company.

f. Data Sharing Agreement

De Los Santos Medical Center must execute a Data Sharing Agreement with the entity, organization or any natural or juridical person to whom personal data of the data subjects of De Los Santos Medical Center are shared or will be shared.

g. Review of Privacy Manual

The DPO with the assistance of the team and other relative employees of the company shall review this Privacy Manual annually. Privacy and security policies and practices within the company shall be updated to remain consistent with current data privacy best practices.

h. Data Privacy Violations of Employees

For the proper implementation and to embed the culture of privacy within the organization the Data Privacy Penalties for Violation is adopted.

B. Physical Security Measures

The DPO with the assistance of the team and other relative employees shall implement procedures to monitor and limit access to the facility containing the personal data, including the activities therein. It shall provide for the actual design of the facility, the physical arrangement of equipment and furniture, the permissible modes of transfer, and the schedule and means of retention and disposal of data, among others. To ensure that mechanical destruction, tampering and alteration of personal data under the custody of the organization are protected from man-made disasters, power disturbances, external access, and other similar threats, provisions like the following must be included in the Manual:

a. Format of data to be collected

The company collects both digital / electronic and paper-based personal data.

b. Storage type and location

Personal data processed by the company are being stored accordingly by the department concerned. Paper-based documents are kept in a locked filing cabinet and fire proof storage vans. Electronic or digital files are stored in the employees' computers, servers and computer systems the company is using, with the assistance and supervision of the IT department.

c. Access procedure of agency personnel

Only authorized personnel shall be allowed in the room or workstation where documents are stored. Proper Privacy Notices to limit access are in place. Other

personnel may be granted access to the files and documents stored by the authorized personnel upon filing of an access request form with the Data Protection Officer and the latter's approval thereof.

d. Monitoring and limitation of access to room or facility

All personnel authorized to enter and access the data room, facility or files and documents must fill out a logbook. They shall indicate the date, time, duration and purpose of each access.

e. Design of office space/work station

Office and work stations, arrangement of furniture and equipment shall provide privacy to anyone processing data. The computers are positioned with considerable spaces between them to maintain privacy and protect the processing of personal data.

f. Persons involved in processing, and their duties and responsibilities

Persons involved in processing shall always maintain confidentiality and integrity of personal data. They are not allowed to bring their own gadgets or storage device of any form when entering their work stations.

g. Use of Electronic Media

Only authorized and company issued electronic media such as desktop, laptop, phone and other storage devices shall be used for the processing of personal data. Only persons authorized by the company shall be allowed to use the company electronic media. Verification and authentication mechanism shall be in place to ensure authority of a person who shall use the company electronic media.

h. Modes of transfer of personal data within the organization, or to third parties

Transfers of personal data via electronic mail shall use a secure email facility with encryption of the data, including any or all attachments. Facsimile technology shall not be used for transmitting documents containing personal data. A privacy and confidentiality notice is properly placed in the email template to oblige the recipient thereof the secured whatever personal data is transfer to him/her.

i. Protection against natural disasters

Room or workstation of those involved in processing of data shall be secured against natural disasters, power disturbances, external access, and other similar threats to prevent mechanical destruction of files and equipment.

j. Retention and disposal procedure

The company shall retain the personal data it holds following the retention schedule provided above. Upon expiration of such period, all physical and electronic copies of the personal data shall be destroyed and disposed of using secure technology. For paper-based files and documents, it shall be destroyed or disposed through shredding to be facilitated by Administrative staff. For electronic-based, it shall be destroyed

or disposed through computer or system deletion to be facilitated by the IT personnel. This activity shall be supervised by the COP and/or the DPO.

C. Technical Security Measures

The appointed DPO, with the assistance of the IT department shall continuously develop and maintain appropriate security policies to safeguard the processing of personal data, particularly the computer network in place, including encryption and/or authentication processes that control and limit access. They include the following, among others:

a. Monitoring for security breaches

The De Los Santos Medical Center, through the IT Department, shall use detection mechanisms to monitor and alert the team of security breaches and/or attempts to interrupt or disturb the system. The IT department shall regularly test and evaluate the company IT infrastructure to see to it that it is properly safeguarded from outside attacks.

b. Security features of the Data Centre, software/s and application/s used

The company, through the IT Department, shall implement reasonable measures to properly secure the Data Center against any unauthorized or malicious access, power disturbances and other calamities. It shall likewise review and evaluate software applications before the installation thereof in computers and devices of the organization to ensure the compatibility of security features with overall operations. The IT department shall check software applications' ability to ensure and maintain the availability, confidentiality and integrity of personal data processed in it.

c. Process for regularly testing, assessment and evaluation of effectiveness of security measures

The organization shall review security policies, conduct vulnerability assessments and perform penetration testing within the company on regular schedule to be prescribed by the appropriate department or unit.

E. Implementation of an Incident response procedure.

The company through its Security Incident Response Team shall observe and follow procedures for the management of personal data breaches, including security incidents. This includes notifications to the National Privacy Commission, Data Subjects, stakeholders and other duties and responsibilities of the Personal Information Controller in managing breach and security incidents.

A. Data Breach Notification

All employees and agents of De Los Santos Medical Center involved in the Processing of Personal Data are tasked with regularly monitoring for signs of a possible data breach or Security Incident.

In the event that such signs are discovered, the employee or agent shall immediately report the facts and circumstances to the DPO within twenty-four (24) hours from his or her discovery for verification as to whether or not a breach requiring notification under the Data Privacy Act has occurred as well as for the determination of the relevant circumstances surrounding the reported

breach and/or Security Incident. The DPO shall notify the National Privacy Commission and the affected Data Subjects pursuant to requirements and procedures prescribed by the DPA. The notification to the National Privacy Commission and the affected Data Subjects shall at least describe the nature of the breach, the Personal Data possibly involved, and the measures taken by the Company to address the breach. The notification shall also include measures taken to reduce the harm or negative consequences of the breach and the name and contact details of the DPO. The form and procedure for notification shall conform to the regulations and circulars issued by the National Privacy Commission, as may be updated from time to time.

B. Breach Reports

All Security Incidents and Personal Data breaches shall be documented through written reports, including those not covered by the notification requirements. In the case of Personal Data breaches, a report shall include the facts surrounding an incident, the effects of such incident, and the remedial actions taken by the Company. In other security incidents not involving Personal Data, a report containing aggregated data shall constitute sufficient documentation. These reports shall be made available when requested by the National Privacy Commission. A general summary of the reports shall be submitted by the DPO to the National Privacy Commission annually.

F. Security Incident Response Procedure

- a) Upon knowledge or when a reasonable belief arises that a security incident or a personal data breach occurred, the person having such knowledge or belief must report it immediately by filling up a Personal Data Breach Form¹ and submit the same to the Data Protection Officer.
- b) The security incident response team headed by the Data Protection Officer shall contact the individual who reported the incident immediately and conduct initial meeting and investigation.
- c) If the occurrence of the data breach affecting personal data is confirmed, the Security Incident Response Policy Procedure activation is warranted and the Data Protection Officer shall contact and ask for the assistance of the Threat Assessment Group.
- d) Within 24 hours from the breach or upon having knowledge of the same, the Data Protection Officer shall initiate a meeting and contact all appropriate database and system administrators and process owners in proper cases, to assist in the investigation effort. The IT Department shall be required to submit an audit trail report, access logs report, or any report which it may deem necessary in the investigation within the same period.
- e) The Data Protection Officer shall direct and coordinate all activities involved with Incident Response Team members in determining the details of the breach. He shall assign a person from the security incident response team who shall be the head of the investigation.
- f) The data protection officer shall identify and contact the appropriate clients, third-party service providers and other stakeholders affected by the breach in coordination with the Legal Consultants of DLSMC.
- g) If the breach occurred at a third party location, the DPO shall determine if a data sharing agreement exist. He shall work with the Legal Consultants of DLSMC and process owners to review contract terms and determine next course of action.

¹ See 7.1 PERSONAL DATA BREACH FORM

- h) The Security Incident Response Team shall work with the appropriate parties to determine the extent of the potential breach. Identify data stored and compromised on all test, development and production systems and see to it that all the appropriate security measures are in place.
- i) Determine the type of personal data that is at risk, including but not limited to:
- Name
 - Signature
 - Age/ Date of Birth
 - Address
 - Citizenship
 - Civil Status
 - Gender / Sexual Life of a person
 - Contact Details
 - Email address
 - Government Identification Numbers
 - Medical and Health Information
 - Privileged Information
 - Specifically established by an executive order or an act of Congress to be kept classified.
- j. The Security Incident Response Team shall determine if there is a breach of sensitive personal information or other information that may, under the circumstances, be used to enable identity fraud; The data is reasonably believed to have been acquired by an unauthorized person; and Either the personal information controller or the NPC believes that the data breach is likely to give rise to a real risk of serious harm to the affected data subject.
- k. If the data involves a.) Information that would likely affect national security, public safety, public order, or public health; b) affects at least one hundred (100) individuals; c) Information required by all applicable laws or rules to be confidential; or personal data of vulnerable groups, the Personal Information Controller shall notify² the National Privacy Commission within 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.
- l. The following information must be included in any Data Breach notification³:
1. **Nature of the Breach.** – There must be, at the very least, a description of: (a) the nature of the breach; (b) a chronology of events, and (c) an estimate of the number of data subjects affected;
 2. **Personal data involved.** – stating the description of sensitive personal information or other information involved.
 3. **Remedial Measures.** – there must be: (a) Description of the measures taken or proposed to be taken to address the breach; (b) Actions being taken to secure or recover the personal data that were compromised; (c) Actions performed or proposed to mitigate possible harm or negative consequences, and limit the damage or distress to those affected by the incident; (d) Action being taken to inform the data subjects affected by the incident, or reasons for any delay in the notification; and (d) the measures being taken to prevent a recurrence of the incident.
 4. **Name and contact details.** – of the Data Protection Officer or contact person designated by the Personal Information Controller to provide additional information.
- m. The Personal Information Controller through its Data Breach Response Team headed by the Data Protection Officer shall also:

² 7.2 DATA SUBJECT MANDATORY PERSONAL DATA BREACH NOTIFICATION

³ 7.5 MANDATORY NOTIFICATION: PERSONAL DATA BREACH REPORT FORM FOR NPC

1. Notify the data subject within **seventy-two (72) hours** upon knowledge of or reasonable belief that a personal data breach has occurred;
 2. The notification may be made on the **basis of available information** within the 72-hour period if the personal data breach is likely to give rise to a real risk to the rights and freedoms of data subjects;
 3. The notification shall have the **same content** as those made to the National Privacy Commission, but shall include instructions on how data subjects will get further information; and
 4. recommendations **regarding how to minimize risks** resulting from breach and to secure any form of assistance.
- n. The notification of affected data subjects shall be done individually, using secure means of communication, whether written or electronic. And whenever individual notification is not possible or would require a disproportionate effort, the personal information controller may seek the approval of the Commission to use alternative means of notification.

G. Annual Reports

De Los Santos Medical Center through its DPO shall be required to submit an Annual Report⁴, where all security incidents and personal data breaches must be documented through written reports, including those not covered by the notification requirements.

In the event of a personal data breach, a report shall include: (a) the facts surrounding the incident; (b) the effects of such incident; and (c) the remedial action taken by the personal information controller. For other security incidents not involving personal data, a report containing aggregated data shall constitute sufficient documentation.

Any or all reports shall be made available when requested by the Commission: Provided, that a summary of all reports shall be submitted to the Commission annually, comprised of general information including the: (1) number of incidents and breach encountered; and (2) classified according to their impact on the availability, integrity, or confidentiality of personal data.

⁴ Annual Security Incident Report

H. Security Incident Response Forms

7.1 Personal Data Breach Report Form

Personal Data Breach Report Form				
Personal Information of Reporting Incident				
Full Name				
Department				
Designation				
Incident Information				
Date Incident was Discovered				
Date of Incident Reporting				
Place of Incident				
Incident Type	Confirmed Breach <input type="checkbox"/>		Suspected Breach <input type="checkbox"/>	
	#	Incident Type		
	1	Loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, USB stick, iPad/tablet device, or paper record)		<input type="checkbox"/>
	2	Equipment theft or failure (e.g. database, application sever failures etc.)		<input type="checkbox"/>
	3	Unauthorized use of, access to or modification of data or information systems		<input type="checkbox"/>
	4	Attempts (failed or successful) to gain unauthorized access to information or IT system(s)		<input type="checkbox"/>
	5	Unauthorized disclosure of sensitive / confidential data		<input type="checkbox"/>
	6	Hacking attack		<input type="checkbox"/>
	7	Unforeseen circumstances such as a fire ,flood , earthquake etc.		<input type="checkbox"/>
	8	Other		<input type="checkbox"/>
1. Nature of Breach				
	a. Description of How the breach occurred.			
	b. Chronology of the events.			

	<div>c. Approximate number of data subjects or records involved</div>		
	<div>d. Description or nature</div>		
	<div>e. Likely consequences</div>		
	<div>a. Description of personal information involved</div>		
2. Data Possibly Involved	<div>b. description of sensitive personal information involved</div>		
	<div>c. description of other information involved</div>		
	<div>a. Description of Measures Taken to Address the Breach</div>		
	<div>b. Actions taken to secure or recover personal data</div>		
3. Remedial Actions Taken	<div>c. Actions performed or proposed to mitigate possible harm</div>		
	<div>d. Actions taken to inform the data subjects <i>*state reason of delay if any</i></div>		
4. Measures taken to prevent recurrence of the incident			

Employee's Confirmation			
Full Name	Signature	Date	
Data Protection Officer Confirmation			
Full Name	Signature	Date	

7.2 Mandatory Personal Data Breach Notification to Data Subjects

De Los Santos Medical Center
201 E Rodriguez Sr. Avenue, Metro Manila, Quezon City
889-DLSMC (35762)

<DATE>
<DATA SUBJECT>
<ADDRESS>

Subject:

<DATA BREACH> dated <DATE> <NPC REGISTRATION NO.>

Dear <DATA SUBJECT>

I write in behalf of <ENTITY>, regarding your data in <BRIEF DESCRIPTION OF DATABASE>.

We regret to inform you that your data has been exposed in this data breach. To our understanding, your exposure is limited to: <DATA INVOLVED IN THE DATA BREACH>.

Nature of the Breach

- Provide a summary of the events that led up to the loss of control over the data. Do not further expose the data subject.
- Describe the likely consequences of the personal data breach.
- Measures taken to Address the Breach.
- Provide information on measures taken or proposed to be taken to address the breach, and to secure or recover the personal data that were compromised.
- Include actions taken to inform affected individuals of the incident. In case the notification has been delayed, provide reasons.
- Describe steps the organization has taken prevent a recurrence of the incident.
- Measures taken to reduce the harm or negative consequences of the breach.
- Describe actions taken to mitigate or limit possible harm, negative consequences, damage or distress to those affected by the incident.
- Assistance to be provided to the affected data subjects.
- Include information on any assistance to be given to affected individuals.

Do not hesitate to contact our Data Protection Officer for further information:

Data Protection Officer

Karl Marxcuz R. Reyes
201 E Rodriguez Sr. Avenue, Metro Manila, Quezon City
krreyes@dlsmc.ph
889-DLSMC (35762) loc. 8828

We commit to provide more information to you as soon as possible, as they become available, with our best efforts.

Sincerely,

De Los Santos Medical Center
Karl Marxcuz R. Reyes

7.3 Summary of Annual Security Incident and Personal Data Breach Reports for PICs

SUMMARY

Annual Security Incident and Personal Data Breach Reports

January to December 2020

Sector: HEALTH City: Quezon City

PERSONAL INFORMATION CONTROLLER

Personal Data Breach, Mandatory Notification	<#>
Personal Data Breach, not covered by mandatory notification requirements	<#>
Other Security Incidents, not amounting to a personal data breach	<#>
Total	<#>

Attack Vectors

How Security Incidents
Occurred

Types	Number	Types	Number
Theft	<#>	Communication Failure	<#>
Fraud	<#>	Fire	<#>
Sabotage/Physical Damage	<#>	Flood	<#>
Malicious Code	<#>	Design Error	<#>
Hacking/Logical Infiltration	<#>	User Error	<#>
Misuse of Resources	<#>	Operations Error	<#>
Hardware Failure	<#>	Software Maintenance Error	<#>
Software Failure	<#>	Third Party Services	<#>
Hardware Maintenance Error	<#>	Others	<#>

Personal Data Breaches

	Confidentiality	Integrity	Availability
Mandatory Notification Required	<#>	<#>	<#>
Mandatory Notification Not Required	<#>	<#>	<#>

PREPAREDBY: _____
DESIGNATION: _____ DATE: _____

7.4 Summary of Annual Security Incident and Personal Data Breach Reports for PIPs

SUMMARY

Annual Security Incident and Personal Data Breach Reports
January to December 2020

PERSONAL INFORMATION PROCESSOR

Security incidents involving personal data processing performed on behalf of PICs	<#>
Personal Data Breaches involving personal data processing performed on behalf of PICs	<#>
Personal Data Breaches reported to PICs	<#>
Total	<#>

Attack Vectors

How Security Incidents Occurred

Types	Number	Types	Number
Theft	<#>	Communication Failure	<#>
Fraud	<#>	Fire	<#>
Sabotage/Physical Damage	<#>	Flood	<#>
Malicious Code	<#>	Design Error	<#>
Hacking/Logical Infiltration	<#>	User Error	<#>
Misuse of Resources	<#>	Operations Error	<#>
Hardware Failure	<#>	Software Maintenance Error	<#>
Software Failure	<#>	Third Party Services	<#>
Hardware Maintenance Error	<#>	Others	<#>

PREPAREDBY: _____
DESIGNATION: _____ DATE: _____

7.5 **Mandatory Notification: Personal Data Breach for the National Privacy Commission**

De Los Santos Medical Center
201 E Rodriguez Sr. Avenue, Metro Manila, Quezon City
889-DLSMC (35762)
<DATE>

<PRIVACY COMMISSIONER>
National Privacy Commission
Pasay City, Metro Manila
Philippines

Subject:

<DATA BREACH> dated <DATE> of <DATABASE> <NPC REGISTRATION NO.>

Gentlemen:

I write in behalf of De Los Santos Medical Center in relation to the data breach of <DATE>, involving <BRIEF DESCRIPTION OF DATA>. This notification is made pursuant to the mandatory data breach notification procedure in Philippine law to the National Privacy Commission.

Responsible Officers. The pertinent details of De Los Santos Medical Center, and the responsible person/s thereof, are as follows:

De Los Santos Medical Center

Karl Marxcuz R. Reyes
201 E Rodriguez Sr. Avenue, Metro Manila, Quezon City
krreyes@dlsmc.ph
889-DLSMC (35762) loc. 8828
Data Protection Officer

<NAME>
<OFFICE ADDRESS>
<E-MAIL ADDRESS>
<TELEPHONE>
<OTHER CONTACT INFO>

Process Owner

<NAME>
<OFFICE ADDRESS>

<E-MAIL ADDRESS>

<TELEPHONE>

<OTHER CONTACT INFO>

Nature of the Breach. In brief, we describe the nature of the incident, thus:

- Describe the nature of the personal data breach.
 - Be as specific as possible. Indicate if the details provided are sensitive to the entity, which may cause unwarranted damage to the entity if disclosed to the public.
 - Provide a chronology that describes how the breach occurred; describe individually the events that led to the loss of control over the personal data.
 - Provide a description of the vulnerability or vulnerabilities that of the data processing system that allowed the breach.
 - Include description of safeguards in place that would minimize harm or mitigate the impact of the personal data breach.
 - Indicate number of individuals or personal records affected. Provide an approximate if the actual impact has not been determined.
 - Describe the likely consequences of the personal data breach. Consider effect on company or agency, data subjects and public.
 - Personal Data Possibly Involved
 - List all sensitive personal information involved, and the form in which they are stored or contained.
 - Also list all other information involved that may be used to enable identity fraud.
- Indicate actions of the organization to minimize/mitigate the effect on the affected individual.

Measures taken to Address the Breach.

- Describe in full the measures that were taken or proposed to be taken to address the breach.
 - Describe how effective these measures are.
 - Indicate whether the data placed at risk have been recovered. Otherwise, provide all measures being taken to secure or recover the personal data that were compromised.
- Provide all actions being performed or proposed to mitigate or limit possible harm, negative consequences, damage or distress to those affected by the incident.
 - Indicate if the affected individuals are aware that the incident has occurred. Include all the actions being taken to inform the data subjects affected by the incident or any reasons for delay in the notification.
 - Describe the steps the organization has taken to prevent a recurrence of the incident.

Should you require further information on this matter, contact us using the information above. Any information that is indicated as unavailable at this time will be determined and reported within five (5) days, or as soon as possible, as they become available.

Sincerely,

De Los Santos Medical Center

<HEAD OF AGENCY/ DATA PROTECTION OFFICER>



INFORMATION CLASSIFICATION POLICY

I. INTRODUCTION

De Los Santos Medical Center (DLSMC) collect, access, use, modify, disclose, retain and dispose vast amount of information. Efficient management of such assets is also necessary to comply with legal and regulatory obligations such as relevant Data Privacy Laws. Different types of information require different protection measures and therefore, applying classification markings of information assets is vital to ensuring effective information security and management. DLSMC acknowledges its responsibility to protect these organizational assets and ensure the confidentiality, integrity and availability of all information within the healthcare institution.

II. OBJECTIVES

The purpose of this policy is to establish a framework for classifying data based on its sensitivity, value and criticality to the organization, so that sensitive corporate and personal data can be secured appropriately. The classification will also:

- raise awareness on the value of DSLMC information;
- provide accountability and appropriate handling for the management and use of information;
- protect information from unauthorized use and disclosure;
- promote the appropriate retention, storage and disposal of data;
- facilitate the disclosure of information and provide protection while in transit;
- assists in complying with legal requirements and obligations such as the Data Privacy Act of 2012;
- enable the appropriate confidentiality, integrity and availability, at the appropriate levels, for identified information; and
- educate all staff of their responsibility to adequately protect information critical to both the hospital and its stakeholders.

Level 3 RESTRICTED	Available only to specified and / or relevant members, with appropriate authorization. A breach of confidentiality could cause serious damage resulting in the compromise of activity within the Hospital from the short to medium term. This includes both personnel data and research data.
LEVEL 2 CONFIDENTIAL	Available only to specified and relevant members, with appropriate authorization. A breach of confidentiality could result in unacceptable damage with very serious and lasting consequences threatening the Hospital or one of its activities.
LEVEL 1 INTERNAL	Available to any authorized member of the Hospital. Typically, if this level of

	information was leaked outside of the, it could be inappropriate.
LEVEL 0 PUBLIC	Available to any member of the public without restriction. This information however should not be placed into the public domain without reason, such as a request or publishing as part of data management policy.

III. SCOPE

This policy applies to any form of data, including paper documents and digital data stored on any type of media. It applies to all of the organization’s employees, as well as to third-party service-providers authorized to access the data.

This policy should be read in conjunction with other DLSMC Data Privacy Policies and Information Security Management Policies and Procedures which are also relevant to the collection, use, disclosure, sharing, retention and destruction of personal data in DLSMC.

IV. DEFINITION OF TERMS

Asset is anything that has value to the organization [ISO/IEC 13335-1:2004]

Anti-Virus Software is a software utility that is designed to prevent, search for, detect and destroy malicious files (ex. viruses, worms, trojan, adware) from a computer.

Confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities, or processes [ISO/IEC 13335-1:2004]

Cryptography is associated with the process of converting ordinary plain text into unintelligible text and vice-versa. It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it.

Data Privacy Act of 2012(DPA) is an act protecting individual personal information in Information and Communications Systems in the Government and the Private Sector, creating for this purpose a National Privacy Commission, and for other purposes.

Data Sharing Agreement refers to a contract, joint issuance, or any similar document that contains the terms and conditions of a data sharing arrangement between two or more parties: Provided, that only personal information controllers shall be made parties to a data sharing agreement;

Encryption is the process of converting (encoding) information from a readable form (plain text) that can be read by everyone into an unreadable form (cipher text) that can only be read by the information owner and other authorized persons. It is a way of safeguarding data, documents, or information from threats such as malicious hackers, spies, criminals.

Firewall is a network security system designed to prevent unauthorized access to or from a private network. It acts as a barrier between a trusted system or network and outside connections, such as the internet.

Information is defined as anything spoken, overheard, written, generated, collected, stored electronically, copied, transmitted or held intellectually concerning DLSMC general business, information systems, employees, business partners, patients.

Information Asset refers to a body or information that has financial value to an organization. (Ex. Strategies, Plans, Trade Secrets, Contracts, Policies, Procedures, Manuals, Memos, etc.).

Integrity the property of safeguarding the accuracy and completeness of assets [ISO/IEC 13335-1:2004]

Non-Disclosure Agreement (NDA) is a legal contract between at least two parties that outlines confidential material, knowledge, or information that the parties wish to share with one another for certain purposes.

Password is a confidential numeric and/or character string used in conjunction with a User ID to verify the identity of the individual attempting to gain access to a computer system.

Personal Data refers to all types of personal information, including privileged information.

Personal Information refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.

Process / Processed / Processing refers to any manual or automated operation or set of operations performed on information including:

- obtaining, recording or keeping the information;
- collecting, organizing, storing, altering or adapting the information;
- retrieving, consulting or using the information;
- disclosing the information or information by transmitting, disseminating or otherwise making it available;
- aligning, combining, blocking, erasing or destroying the information.

Sensitive Personal Information refers to the following personal information:

- | | |
|--|--------------------------------------|
| - Race, Ethnic origin, Color | - Age |
| - Marital status | - Previous or Current Health Records |
| - Education | - Genetic or sexual life |
| - Licenses | - Tax Returns |
| - Social Security Number | - Issued by Government Agencies |
| - Religious, philosophical or political affiliations | |

Third Party Service Provider refers to any individual or commercial company that have been contracted by DLSMC to provide goods and/or services (ex. project/contract management, consultancy, information system development and/or support, supply and/or support of computer software/hardware, equipment maintenance, information management services, patient/client care and management services) to DLSMC.

V. ROLES AND RESPONSIBILITIES

It is the responsibility of all DLSMC employees to ensure that all information (structured and unstructured data, paper based and electronic) is classified appropriately and apply the relevant procedures pertaining to that classification at all times.

1.) Information Asset Owners

Information Asset Owners are responsible for:

- The full implementation of this policy and all other relevant policies with in DLSMC;
- Ensuring all information (irrespective of its format) owned, created, received and processed within DLSMC is classified and handled in accordance with this policy;
- Making sure adequate procedures are implemented within DLSMC, so as to ensure DLSMC staff, interns and third party service providers are made aware of, and are instructed to comply with this policy and all other relevant policies;
- Making sure adequate procedures and training programs are implemented within DLSMC to ensure on-going compliance of this policy and all other relevant policies.

2.) Department Managers

Department Managers are responsible for:

- The implementation of this policy and all other relevant DLSCM policies within their department;
- Ensuring all information (irrespective of its format) owned, created, received, stored and processed within DLSCM is classified and handled in accordance with this policy;
- Ensuring that all department staff, interns and third party service providers are made aware of, understand and have access to this policy and all other relevant DLSCM policies.
- Ensuring that all department staff, interns and third-party service providers are instructed to comply and are provided with adequate information and training regarding the implementation of this policy and all other relevant DLSCM policies;
- Consulting with HR Department in relation to the appropriate procedures to follow when a breach of this policy has occurred.

3.) DLSCM Staff

Each Staff member is responsible for:

- Complying with the terms of this policy and all other relevant DLSCM policies, procedures, regulations, and applicable legislation;
- Ensuring all information (irrespective of its format) is classified and handled in accordance with this policy;
- Reporting all misuse and breaches of this policy to their Department Manager.

4.) Third Party Service Providers

Each third party services providers are responsible for:

- Complying with the terms of this policy and all other relevant DLSCM policies, procedures, regulations, and applicable legislation;
- Ensuring all information (irrespective of its format) is classified and handled in accordance with this policy;
- Reporting all misuse and breaches of this policy to the Department Manager where they provide their service.

VI. POLICY

1. Information Classification

All information (irrespective of its format) owned, created, collected and further processed by DLSCM must be classified according to the sensitivity of its contents. Classification controls should take account of the organizational needs for sharing or restricting the information and the associated impacts and risks (ex. consequences if information is handled inappropriately). All information owned, created, collected, or processed by DLSCM must be classified into one of the following categories:

- 1.1. **Public Information** is defined as information that is available to the general public and is intended for distribution or disclosure outside DLSCM. There would be no impact on DLSCM, its staff, clients or patients if this type of information was mishandled or accidentally disclosed. Some examples of public information include:
 - Patient/Client brochures;
 - News or media releases;
 - Advertisements;
 - Web content;
 - Job postings;
 - Public Health Information;

- Pamphlets containing general information regarding services offered by DLSMC;
- Principal Hospital contacts e.g. name/email address, telephone numbers for public –facing roles or made freely available.

1.2. **Internal Information** is defined as information that is only intended for internal distribution among DLSMC staff and authorized third party service providers. In most instances there would be no significant impact on DLSMC, its staff, clients or patients if this type of information was mishandled or accidentally released. Some examples of Internal information include:

- Internal Telephone Directory and email addresses.
- User manuals;
- Training manuals and documentation;
- Inter-office memorandums (depending on the content)
- Department Policies and Procedures
- Data that is already in the public domain but was not intended as such and could result in litigation if republished.

1.3. **Confidential Information** is defined as information which is protected by DLSMC policies or legal contracts or by the Data Privacy Act of 2012 and other legislation or regulations. The unauthorized or accidental disclosure of this information could adversely impact DLSMC, its patients, its staff and its business partners. Some examples of confidential information include:

- Passwords / cryptographic private keys;
- Patient / Staff Personal Information (except that which is restricted);
- Highly sensitive data that will explicitly identify individuals which, if disclosed, puts the individual at risk from identity theft, direct profiling and marketing threats from criminal or vigilante individuals or organizations;
- Financial information regarding individuals e.g. payment information (credit card details), bank account details, information about indebtedness (medical fees/bills);
- Government Licenses and Permits
- Medico-Legal and other regulatory cases
- Unpublished medical research;
- Policies and Procedures (except those published on the website);
- Financial Information / budgetary reports;
- Draft reports, Audit reports;
- Purchasing Information;
- Interdepartmental Policies and Procedure
- Vendor contracts / commercially sensitive information;
- Information covered by non-disclosure / confidentiality agreements;
- Information collected as part of criminal / HR Investigations;
- Incident reports;
- Business Continuity Plans.

1.4. **Restricted Information** is defined as highly sensitive confidential information. The unauthorized or accidental disclosure of this information would seriously and adversely impact DLSCMC, its patients, staff and its business partners. Some examples of restricted information include:

- Patient / Staff sensitive personal information;
- Patient / Staff medical records;
- Unpublished financial report;
- Business-sensitive data such as detailed financial records, information on commercial contracts;
- Internal correspondence, timesheets, expenses.
- Strategic corporate plans;
- Sensitive medical research;
- Doctor-patient privileged information;
- Incomplete reports and other documents whose integrity may be damaged by uncontrolled/unauthorized changes, or whose leakage may cause damage to the project, the project funders or the Hospital.

2. Information Handling

All Information (irrespective of its format) owned, created, collected and further processed by DLSCMC must be handled appropriately according to its classification. The Information Handling Matrix specifies how the different classifications of information must be handled is found in the Appendix section of this policy.

Processing of Information containing Personal Data should be in accordance with the DLSCMC Data Privacy Manual

3. Information Classification Process

To classify Information Assets, the following must be performed:

- 3.1. Create an Information Asset Inventory by identifying all information to be classified.
- 3.2. Perform classification of information based on the Information Classification stated in this policy.
- 3.3. Label the classified Information.
- 3.4. Implement the Information Handling.

VII. RELEVANT POLICIES

Data Privacy Manual
Security Incident Response Policy and Procedure
Password Policy and Guidelines
Back Up Policy
Acceptable Use Policy
Email and Communication Policy
Clean Desk Policy
Clear Screen Policy

VIII. RELEVANT LEGISLATION

Health Privacy Code of 2016
Data Privacy Act of 2012
National Archives of the Philippines Act of 2007
RA 11332 or the Law On Reporting of Communicable Diseases
Philippine AIDS Prevention and Control Act of 1998
Anti-Violence Against Women and Their Children Act of 2004

IX. ENFORCEMENT

Any person found to have violated this policy may be subjected to disciplinary action based on the DPA Penalties for Violation and on the Penalties stated in Chapter VIII of the Data Privacy Act of 2012.

X. APPENDIX

Information Handling Matrix

- a. Storage of Electronic-Based Information
- b. Storage of Paper-Based Information
- c. Transmission of Information
- d. Physical Security
- e. Disposal of Information

DLSMC Information Classification Matrix				
Item	Public	Internal	Confidential	Restricted
Definition	Information that is available to the general public and is intended for distribution outside DLSMC.	Information that is only intended for internal distribution among DLSMC staff and authorized third party service providers.	Information which is protected by DLSMC policies or legal contracts or by the Data Privacy Act of 2012 and other legislation or regulations.	Highly sensitive confidential information.
Examples	<ul style="list-style-type: none"> • Patient/Client brochures; • News or media releases; • Pamphlets; • Advertisements; • Web content; • Job postings; • Public Health Information. • Principal Hospital contacts e.g. name/email address, telephone numbers for public –facing roles or made freely available. 	<ul style="list-style-type: none"> • Internal Telephone Directory and email addresses. • User manuals; • Training manuals and documentation; • Inter-office memorandums (depending on the content) • Department Policies and Procedures • Data that is already in the public domain but was not intended as such and could result in litigation if republished. 	<ul style="list-style-type: none"> • Passwords / cryptographic private keys; • Patient / Staff Personal Information (except that which is restricted); • Highly sensitive data that will explicitly identify individuals which, if disclosed, puts the individual at risk from identity theft, direct profiling and marketing threats from criminal or vigilante individuals or organizations; • Financial information regarding individuals e.g. payment information (credit card details), bank account details, information about indebtedness (medical fees/bills); • Government Licenses and Permits • Medico-Legal and other regulatory cases • Unpublished medical research; • Policies and Procedures (except those published on the website); • Financial Information / budgetary reports; • Draft reports, Audit reports; • Purchasing Information; • Interdepartmental Policies and Procedure • Vendor contracts / commercially sensitive information; • Information covered by non-disclosure / confidentiality agreements; • Information collected as part of criminal/HR Investigations; • Incident reports; • Business Continuity Plans. 	<ul style="list-style-type: none"> • Patient / Staff sensitive personal information; • Patient / Staff medical records; • Unpublished financial report; • Business-sensitive data such as detailed financial records, information on commercial contracts; • Internal correspondence, timesheets, expenses. • Strategic corporate plans; • Sensitive medical research; • Doctor-patient privileged information; • Incomplete reports and other documents whose integrity may be damaged by uncontrolled/unauthorized changes, or whose leakage may cause damage to the project, the project funders or the Hospital.
Consequences if Information is mishandled	None	In most instances there would be no significant impact on DLSMC, its staff, clients or patients.	<p>Unauthorized or accidental disclosure of this information could adversely impact DLSMC, its patients, its staff and its business partners.</p> <p>May result to violations which may subject DLSMC, its employees and stakeholders to legal sanctions and penalties provided for by law</p>	<p>Unauthorized or accidental disclosure of this information would seriously and adversely impact DLSMC, its patients, staff and its business partners.</p> <p>May result to violations which may subject DLSMC, its employees and stakeholders to legal sanctions and penalties provided for by law.</p>

DLSMC Information Handling Matrix				
Item	Public	Internal	Confidential	Restricted
Document Marking	No marking required.	No marking required.	All pages of the document to be clearly marked “Confidential” in the footer section of the page or stamped appropriately.	All pages of the document to be clearly marked “Restricted” in the footer section of the page or stamped appropriately.
Printing, Scanning and Photocopying	No special precautions required.	No special precautions required.	Printing, scanning and photocopying of Confidential Information must be kept to a minimum and only when absolutely necessary. 1) Printers, Scanners and Photocopiers should be located within an area which is not accessible by the general public. 2) Always ensure original documents and copies are removed from printer, scanner or photocopier as soon as possible.	Printing, scanning and photocopying of Restricted Information must be kept to a minimum and only when absolutely necessary. 1) Printers, Scanners and Photocopiers should be located within an area which is not accessible by the general public. 2) Always ensure original documents and copies are removed from printer, scanner or photocopier as soon as possible.
Backup and Recovery	Backed up weekly & backup tapes should be stored in a safe location when not in use.	Backed up weekly & backup tapes should be stored in a safe location when not in use.	Backed up daily, preferably onto a secure network server. If backed up locally onto a backup tape instead of a server, then the backup tapes must be stored in a secured location such as a locked filing cabinet, drawer or a safe when not in use. The backup should be tested at least once a month to ensure you can recover the information from the backup tapes in the event of a system crash or by accidental or natural disasters.	Backed up daily, preferably onto a secure network server. If backed up locally onto a backup tape instead of a server, then the backup tapes must be stored in a secured location such as a locked filing cabinet, drawer or a safe when not in use. The backup should be tested at least once a month to ensure you can recover the information from the backup tapes in the event of a system crash or by accidental or natural disasters.
DLSMC Information Handling Matrix				
Item	Public	Internal	Confidential	Restricted
Access to / disclosure of the information	Available to the general public	Generally made available to all staff, third party service providers on a need to know basis	Confidential information must only be accessible on a need to know basis. Confidential information must only be: 1) Accessible to DLSMC staff who have a valid business need to access the information or have been authorized to access the information by the designated DLSMC Information Asset Owner. 2) Released and disclosed to third parties external to DLSMC (including regulatory	Restricted information must only be accessible on a need to know basis. Restricted information must only be: 1) Accessible to DLSMC staff who have a valid business need to access the information or have been authorized to access the information by the designated DLSMC Information Asset Owner. 2) Released and disclosed to third parties external to DLSMC (including regulatory agencies and government agencies) in accordance with the relevant legislation (Data Privacy Act of 2012).

			agencies and government agencies) in accordance with the relevant legislation (Data Privacy Act of 2012). 3) Processed by third party service providers who have a legal contract in place with DLSMC to provide information management services and have signed a <i>Non-Disclosure Agreement</i> with DLSMC or <i>Data Sharing Agreement</i> if it involves Personal Data.	3) Processed by third party service providers who have a legal contract in place with DLSMC to provide information management services and have signed a <i>Non-Disclosure Agreement</i> with DLSMC or <i>Data Sharing Agreement</i> if it involves Personal Data.
DLSMC Information Handling Matrix				
Item	Public	Internal	Confidential	Restricted
Publication on the Internet	Public information which is to be published on Internet sites must be authorized by DLSMC Marketing or PIC.	Internal information which is to be published on Internet sites must be authorized by DLSMC Marketing or PIC.	Confidential Information must never be published, posted or discussed on any internet sites including those sites which are officially sanctioned by DLSMC (such as but not limited to any social media sites, chat rooms, DLSMC website).	Restricted Information must never be published, posted or discussed on any internet sites including those sites which are officially sanctioned by DLSMC (such as but not limited to any social media sites, chat rooms, DLSMC website).
Breach of Confidentiality <ul style="list-style-type: none">• Theft or loss of information• Loss / Theft of a computer device containing the information• Actual or suspected unauthorized access• Accidental or unauthorized disclosure	No special requirements.	No special requirements.	All information breaches involving the actual or suspected loss, theft or disclosure of confidential information must be reported and handled in accordance with the <i>DLSMC Security Incident Response Policy and Procedure</i> .	All information breaches involving the actual or suspected loss, theft or disclosure of confidential information must be reported and handled in accordance with the <i>DLSMC Security Incident Response Policy and Procedure</i>

DLSMC Storage of Electronic-Based Information				
Item	Public	Internal	Confidential	Restricted
DLSMC Network Server	No special precautions required.	No special precautions required.	<ol style="list-style-type: none">1) Confidential Information and DLSMC Information Systems that store or process such information should be stored/hosted on a DLSMC Network Server and not stored locally on the hard drive of a laptop or desktop computer.2) Confidential Information stored on a DLSMC network server which is not stored as part of any DLSMC Information Systems, must be held within a secure folder which is only accessible by an authorized DLSMC staff.3) The Network Server must have an installed Firewall and is regularly updated.	<ol style="list-style-type: none">1) Restricted Information and DLSMC Information Systems that store or process such information should be stored/hosted on a DLSMC Network Server and not stored locally on the hard drive of a laptop or desktop computer.2) Restricted Information stored on a DLSMC network server which is not stored as part of any DLSMC Information Systems, must be held within a secure folder which is only accessible by an authorized DLSMC staff.3) The Network Server must have an installed Firewall and is regularly updated.
Desktop Computer	No special precautions required.	No special precautions required.	<p>Strictly prohibited except where the:</p> <ol style="list-style-type: none">1) Storage is necessary for business or technical reasons and,2) Desktop computer is password protected in accordance with the <i>DLSMC Password Policy and Guidelines</i> and,3) Anti-virus software should be installed, enabled and regularly updated.4) Information is backed up on a regular basis.	<p>Strictly prohibited except where the:</p> <ol style="list-style-type: none">1) Storage is necessary for business or technical reasons and,2) Desktop computer is password protected in accordance with the <i>DLSMC Password Policy and Guidelines</i> and,3) Anti-virus software should be installed, enabled and regularly updated.4) Information is backed up on a regular basis.

DLSMC Storage of Electronic-Based Information				
Item	Public	Internal	Confidential	Restricted
Laptop Computer	No special precautions required.	No special precautions required.	Strictly prohibited except where the: <ol style="list-style-type: none">1) Storage is necessary for business or technical reasons and,2) Laptop computer is password protected in accordance with the <i>DLSMC Password Policy and Guidelines</i> and,3) Anti-virus software should be installed and enabled.4) Information is backed up on a regular basis.	Strictly prohibited except where the: <ol style="list-style-type: none">1) Storage is necessary for business or technical reasons and,2) Laptop computer is password protected in accordance with the <i>DLSMC Password Policy and Guidelines</i> and,3) Anti-virus software should be installed and enabled.4) Information is backed up on a regular basis.
Mobile Computing Device <ul style="list-style-type: none">• Smart Phones• Tablets• Notebook computers	No special precautions required.	No special precautions required.	Strictly prohibited except where the: <ol style="list-style-type: none">1) Storage is necessary for business or technical reasons and,2) Anti-virus software should be installed and enabled.3) Information is backed up on a regular basis.	Strictly prohibited except where the: <ol style="list-style-type: none">1) Storage is necessary for business or technical reasons and,2) Anti-virus software should be installed and enabled.3) Information is backed up on a regular basis.

DLSMC Storage of Electronic-Based Information				
Item	Public	Internal	Confidential	Restricted
Removable Storage Devices <ul style="list-style-type: none">• CD/DVD• Floppy Disks• External/Portable Hard Drive• USB Storage Devices	No special precautions required.	No special precautions required.	Strictly prohibited except where the: 1) Storage is necessary for business or technical reasons and, 2) Information is backed up on a regular basis. Only DLSMC-approved USB Storage Device may be used to store or transfer DLSMC Information.	Strictly prohibited except where the: 1) Storage is necessary for business or technical reasons and, 2) Information is backed up on a regular basis. Only DLSMC-approved USB Storage Device may be used to store or transfer DLSMC Information.
Photographic or Video Recording Device <ul style="list-style-type: none">• Digital Cameras• Video Cameras• Any devices which are capable of taking still or video recording	No special precautions required.	No special precautions required.	1) Photographic and video recordings taken as part of patient treatment and care must be transferred from the photographic or video recording device onto the department local network server or to the DLSMC network server as soon as practical. When the transfer is complete, the photographic/video recording on the device should be deleted 2) In the event that this cannot be carried out immediately, the photographic or video recording device should be locked away securely when not in use.	1) Photographic and video recordings taken as part of patient treatment and care must be transferred from the photographic or video recording device onto the DLSMC network server as soon as practical. When the transfer is complete, the photographic/video recording on the device should be deleted. 2) In the event that this cannot be carried out immediately, the photographic or video recording device should be locked away securely when not in use.

DLSMC Storage of Electronic-Based Information				
Item	Public	Internal	Confidential	Restricted
Audio Recording Devices <ul style="list-style-type: none">Tape recordersAny device which is capable of taking audio recordings	No special precautions required.	No special precautions required.	1) Audio recordings taken as part of patient treatment and care must be transferred from the audio recording device onto the DLSMC network server as soon as practical. When the transfer is complete, the audio recording on the device should be deleted. 2) When the audio recordings have been transferred to a DLSMC Network Server, all local copies stored on the audio recording device should be deleted.	1) Audio recordings taken as part of patient treatment and care must be transferred from the audio recording device onto the DLSMC network server as soon as practical. When the transfer is complete, the audio recording on the device should be deleted. 2) When the audio recordings have been transferred to a DLSMC Network Server, all local copies stored on the audio recording device should be deleted.
Staff personal devices or Bring Your Own Device (BYOD). Where the device is the staff member's personal property and is not owned or leased by DLSMC)	No special precautions required.	No special precautions required.	Storage may be allowed but the use, retention and storage of such information is subject to BYOD Policy.	Storage may be allowed but the use, retention and storage of such information is subject to BYOD Policy.
Third-party off-site storages. Where the storage of information has been outsourced to a third party company.	No special precautions required.	No special precautions required.	Confidential Information may only be hosted and stored off-site by third parties, provided the third party has signed a <i>Non-Disclosure Agreement</i> and a <i>Data Sharing Agreement</i> with DLSMC.	Restricted Information may only be hosted and stored off-site by third parties, provided the third party has signed a <i>Non-Disclosure Agreement</i> and <i>Data Sharing Agreement</i> with DLSMC.

DLSMC Storage of Electronic-Based Information				
Item	Public	Internal	Confidential	Restricted
Email messages	No special precautions required.	No special precautions required.	<p>Confidential Information which is received via email should not remain permanently on a local computer once it has been read by the intended recipient.</p> <ol style="list-style-type: none">1) Once the email has been read, the Confidential Information contained within the email message should be moved to a secure folder (with restricted access) on the DLSMC Network Server.2) When the information has been moved to the server, all local copies of the email message should be deleted (i.e. delete the copy of the email message in your email inbox and ensure you empty the contents of deleted email folder).3) Alternatively, the email message and/or the Confidential Information may be printed out and stored away in a secure manner (i.e. stored in a locked filing cabinet or a secure lockable area with restricted access).	<p>Restricted Information which is received via email should not remain permanently on a local computer once it has been read by the intended recipient.</p> <ol style="list-style-type: none">1) Once the email has been read, the Restricted Information contained within the email message should be moved to a secure folder (with restricted access) on the DLSMC Network Server.2) When the information has been moved to the server, all local copies of the email message should be deleted (i.e. delete the copy of the email message in your email inbox and ensure you empty the contents of deleted email folder).3) Alternatively, the email message and/or the Restricted Information may be printed out and stored away in a secure manner (i.e. stored in a locked filing cabinet or a secure lockable area with restricted access).

DLSMC Storage of Paper-Based Information				
Item	Public	Internal	Confidential	Restricted
Paper documents and other printed materials	No special precautions required.	Reasonable precautions to prevent the risk of deterioration, loss and access by unauthorized third parties.	<p>The information must be stored in such a way to ensure it is protected against:</p> <ol style="list-style-type: none">1) Unauthorized access. The information should be locked away in a filing cabinet, drawer or safe or records room when not in use.2) Protect or afford appropriate security measures against environmental hazard (ex. Fire, flooding, temperature, humidity, atmospheric pollution, etc.).3) Proper storage and sorting must be observed to protect such from deterioration and/or loss.	<p>The information must be stored in such a way to ensure it is protected against:</p> <ol style="list-style-type: none">1) Unauthorized access. The information should be locked away in a filing cabinet, drawer or safe or records room when not in use.2) Protect or afford appropriate security measures against environmental hazard (ex. Fire, flooding, temperature, humidity, atmospheric pollution, etc.).3) Proper storage and sorting must be observed to protect such from deterioration and/or loss.
Transmission of Information				
Item	Public	Internal	Confidential	Restricted
<p>Spoken word</p> <ul style="list-style-type: none">• Conversations• Meetings• Telephone/mobile calls	No special precautions required.	No special precautions required.	<ol style="list-style-type: none">1) Confidential Information should only be discussed with authorized individuals within a private setting.2) Avoid discussion in public areas such as elevators, hallways, staircases, cafeterias, etc.3) If confidential information is necessary to be communicated on the phone, ensure that the person in the other line is certainly identified as that person intended to be.	<ol style="list-style-type: none">1) Restricted Information should only be discussed with authorized individuals within a private setting.2) Avoid discussion in public areas such as elevators, hallways, staircases, cafeterias, etc.3) If restricted information is necessary to be communicated on the phone, ensure that the person in the other line is certainly identified as that person intended to be.
Electronic File Transfer	No special handling required.	No special handling required.	<ol style="list-style-type: none">1) Transmission must be authorized by the Department Head, IT Department Head and the DPO.2) Information transfer must take place via a secured channel (ex. Secure FTP, TLS, VPN, etc.)	<ol style="list-style-type: none">1) Transmission must be authorized by the Department Head, IT Department Head and the DPO.2) Information transfer must take place via a secured channel (ex. Secure FTP, TLS, VPN, etc.)
Text Message (SMS)	No special handling required.	No special handling required.	Under no circumstances whatsoever should Confidential Information be transmitted by text.	Under no circumstances whatsoever should Restricted Information be transmitted by text.
Transmission of Information				

Item	Public	Internal	Confidential	Restricted
Internal Post/Correspondence	No special handling required.	No special handling required.	<p>Standard Internal Postal Procedure:</p> <ol style="list-style-type: none"> 1) If possible, notify recipient in advance. 2) Ensure you have the correct name and address of the intended recipient on the envelope. 3) Send in a sealed inter-office envelope marked “CONFIDENTIAL”. <p>Removable Storage Media:</p> <p>All CDs, DVDs, diskettes, tapes and other removable storage media containing Confidential Information must be password protected.</p> <p>A process must be in place to ensure the appropriate disposal of the information on the removable storage media once the transfer is complete.</p>	<p>Standard Internal Postal Procedure:</p> <ol style="list-style-type: none"> 1) If possible, notify recipient in advance. 2) Ensure you have the correct name and address of the intended recipient on the envelope. 3) Send in a sealed inter-office envelope marked “RESTRICTED”. <p>Removable Storage Media:</p> <p>All CDs, DVDs, diskettes, tapes and other removable storage media containing Restricted Information must be password protected A process must be in place to ensure the appropriate disposal of the information on the removable storage media once the transfer is complete.</p> <p>A process must be in place to ensure the appropriate disposal of the information on the removable storage media once the transfer is complete.</p>
Transmission of Information				
Item	Public	Internal	Confidential	Restricted
External Post	No special handling required.	No special handling required.	<p>Standard External Post Procedure:</p> <ol style="list-style-type: none"> 1) If possible, notify recipient in advance. 2) Ensure that the correct name and address of the intended recipient is on the envelope. 3) Send in a sealed envelope marked “CONFIDENTIAL” and add on a return address where this will not compromise privacy. 4) A <i>Confidentiality Notice</i> must be visible outside the sealed envelope. 	<p>Standard External Post Procedure:</p> <ol style="list-style-type: none"> 1) If possible, notify recipient in advance. 2) Ensure that the correct name and address of the intended recipient on the envelope. 3) Send in a sealed envelope marked “RESTRICTED” and add on a return address where this will not compromise privacy. 4) A <i>Confidentiality Notice</i> must be visible outside the sealed envelope. 5) Send by normal post. <p>Removable Storage Media:</p>

			<p>5) Send by normal post.</p> <p>Removable Storage Media:</p> <p>All CDs, DVDs, diskettes, tapes and other removable storage media containing Confidential Information must be password-protected.</p> <p>A process must be in place to ensure the appropriate disposal of the information on the removable storage media once the transfer is complete.</p> <p>Bulk Postal procedure:</p> <p>When sending bulk confidential information by post to the same address, you must use an approved courier or a registered postal service.</p>	<p>All CDs, DVDs, diskettes, tapes and other removable storage media containing Confidential Information must be password protected.</p> <p>A process must be in place to ensure the appropriate disposal of the information on the removable storage media once the transfer is complete.</p> <p>Bulk Postal procedure:</p> <p>When sending bulk confidential information by post to the same address, you must use an approved courier or a registered postal service.</p>
Transmission of Information				
Item	Public	Internal	Confidential	Restricted
Internal Email (email address ending in @dlsmc.ph)	No special handling required.	No special handling required.	<ol style="list-style-type: none"> 1) Ensure that the name and email address of the intended recipient is correct. 2) The email message is clearly marked as “Confidential”. 3) Only the minimum amount of Confidential Information as is necessary for a given function(s) to be carried out is to be sent. 4) Only DLSMC Outlook Email Account shall be used in transmitting email with confidential information. 5) The email attachments must be password-protected file. Read and Delivery Request in the message options must be enabled. 	<ol style="list-style-type: none"> 1) Ensure that the name and email address of the intended recipient is correct. 2) The email message is clearly marked as “Restricted”. 3) Only the minimum amount of Restricted Information as is necessary for a given function(s) to be carried out is to be sent. 4) Only DLSMC Outlook Email Account shall be used in transmitting email with confidential information. 5) The email attachments must be password-protected. Read and Delivery Request in the message options must be enabled.

External Email (email address not ending in @dlsmc.ph)	No special handling required.	No special handling required.	<ol style="list-style-type: none"> 1) The information transfer must be legally justifiable in accordance with the Data Privacy Act of 2012. 2) Ensure that the name and email address of the intended recipient is correct. 3) The email must consist of a title in the subject line to include the word “Confidential” and have an appropriate email disclaimer at the end of the email message. 4) All Confidential Information attached in the email is password-protected. 5) If the email contains Personal Information, the <i>DLSMC Authorization and Agreement to Send Personal Data by Email</i> must be completed by the requestor. 	<ol style="list-style-type: none"> 1) The information transfer must be legally justifiable in accordance with the Data Privacy Act of 2012. 2) Ensure that the name and email address of the intended recipient is correct. 3) The email must consist of a title in the subject line to include the word “Restricted” and have an appropriate email disclaimer at the end of the email message. 4) All Restricted Information attached in the email message is password-protected. 5) If the email contains Sensitive Personal Information, the <i>DLSMC Authorization and Agreement to Send Personal Data by Email</i> must be completed by the requestor.
--	-------------------------------	-------------------------------	--	--

Transmission of Information				
Item	Public	Internal	Confidential	Restricted
Fax Message	Use standard <i>DLSMC Fax Cover Sheet</i> and take reasonable care in dialing the fax number.	<ol style="list-style-type: none"> 1) Use standard <i>DLSMC Fax Cover Sheet</i> and take reasonable care in dialing the fax number. <p>Should not be sent from a fax machine which is located within an area that is accessible to the general public.</p>	<p>In accordance with the <i>DLSMC Email and Communication Policy</i>, Confidential Information should only be sent by fax in exceptional circumstances such as:</p> <ol style="list-style-type: none"> a) Medical Emergency, b) Where a legal obligation exists, c) Informed consent. <p>When Confidential Information has to be sent by fax:</p>	<p>In accordance with the <i>DLSMC Email and Communication Policy</i>, Restricted Information should only be sent by fax in exceptional circumstances such as:</p> <ol style="list-style-type: none"> a) Medical Emergency, b) Where a legal obligation exists, c) Informed consent.

Fax Message	Use standard <i>DLSMC Fax Cover Sheet</i> and take reasonable care in dialing the fax number.	2) Use standard <i>DLSMC Fax Cover Sheet</i> and take reasonable care in dialing the fax number. 3) Should not be sent from a fax machine which is located within an area that is accessible to the general public.	1) The fax machine used to send/receive Confidential Information should be located within a secured area which is not accessible by the general public. 2) Make sure you are using the correct fax number for the intended recipient. 3) Ensure the <i>DLMSC Fax Cover Sheet</i> is used. 4) Where possible, you should call the intended recipient by phone before transmission to ensure the message will be retrieved immediately upon transmission. Subsequent phone call must be made to confirm receipt of transmission. 5) Ensure that there are no documents from the fax machine after every use.	When Restricted Information has to be sent by fax: 1) The fax machine used to send/receive Restricted Information should be located within a secured area which is not accessible by the general public. 2) Make sure you are using the correct fax number for the intended recipient. 3) Ensure the <i>DLMSC Fax Cover Sheet</i> is used. 4) Where possible, you should call the intended recipient by telephone before transmission to ensure the message will be retrieved immediately upon transmission. Subsequent telephone call must be made to confirm receipt of transmission. 5) Ensure that there are no documents from the fax machine after every use.
-------------	---	--	--	--

Physical Security				
Item	Public	Internal	Confidential	Restricted
Office / Workplace	No special precautions required.	No special precautions required.	1) Access to areas containing Confidential Information should be restricted to authorized staff only (ex. manned reception desk, access to areas controlled via biometrics). 2) Where practical, <i>DLSMC Clean Desk Policy</i> should be in operation where all Confidential Information (irrespective of format) is cleared from desks and locked away securely when it is not in use.	1) Access to areas containing Restricted Information should be restricted to authorized staff only (ex. manned reception desk, access to areas controlled via biometrics). 2) Where practical, <i>DLSMC Clean Desk Policy</i> should be in operation where all Restricted Information (irrespective of format) is cleared from desks and locked away securely when it is not in use.

Desktop Computers	Desktop computers must be: 1.) Password protected in accordance with the <i>DLSMC Password Policy and Guidelines</i> , 2.) Logged off or “screen-locked” in accordance with the <i>DLSMC Clear Screen Policy</i> . 3.) USB Ports must be disabled for USB Storage Devices.	Desktop computers must be: 1.) Password protected in accordance with the <i>DLSMC Password Policy and Guidelines</i> , 2.) Logged off or “screen-locked” in accordance with the <i>DLSMC Clear Screen Policy</i> . 3.) USB Ports must be disabled for USB Storage Devices.	Desktop computers must be: 1.) Password protected in accordance with the <i>DLSMC Password Policy and Guidelines</i> . 2.) Logged off or “screen-locked” in accordance with the <i>DLSMC Clear Screen Policy</i> . 3.) USB Ports must be disabled for USB Storage Devices. 4.) Positioned in such a way as to minimize the risk of unauthorized disclosure or viewing information displayed on the screen or unauthorized access by unauthorized individuals.	Desktop computers must be: 1.) Password protected in accordance with the <i>DLSMC Password Policy and Guidelines</i> . 2.) Logged off or “screen-locked” in accordance with the <i>DLSMC Clear Screen Policy</i> . 3.) USB Ports must be disabled for USB Storage Devices. 4.) Positioned in such a way as to minimize the risk of unauthorized disclosure or viewing information displayed on the screen or unauthorized access by unauthorized individuals.
Physical Security				
Item	Public	Internal	Confidential	Restricted
Laptop Computers	Laptop computers must be: 1.) Password protected in accordance with the <i>DLSMC Password Policy and Guidelines</i> . 2.) Stored in a locked drawer or cabinet if left in the office overnight 3.) USB Ports must be disabled for USB Storage Devices. 4.) Kept with the user at all times when working off-site.	Laptop computers must be: 1.) Password protected in accordance with the <i>DLSMC Password Policy and Guidelines</i> . 2.) Logged off or “screen-locked” in accordance with the <i>DLSMC Clear Screen Policy</i> . 3.) Stored in a locked drawer or cabinet if left in the office overnight. 4.) USB Ports must be disabled for USB Storage Devices.	Laptop computers must be: 1.) Password protected in accordance with the <i>DLSMC Password Policy and Guidelines</i> . 2.) Logged off or “screen-locked” in accordance with the <i>DLSMC Clear Screen Policy</i> . 3.) Stored in a locked drawer or cabinet if left in the office overnight. 4.) USB Ports must be disabled for USB Storage Devices.	Laptop computers must be: 1.) Password protected in accordance with the <i>DLSMC Password Policy and Guidelines</i> . 2.) Logged off or “screen-locked” in accordance with the <i>DLSMC Clear Screen Policy</i> . 3.) Stored in a locked drawer or cabinet if left in the office overnight. 4.) USB Ports must be disabled for USB Storage Devices.

		5.) Kept with the user at all times when working off-site.		
Physical Security				
Item	Public	Internal	Confidential	Restricted
Mobile Computing Devices <ul style="list-style-type: none">Smart PhonesTabletsPDAs	Mobile computing devices must be: 1.) Kept with the user at all times when working off-site. 2.) Locked away in a filing cabinet or drawer when left in the office overnight. 3.) Lock screen must be enabled when not in use.	Mobile computing devices must be: 1.) Kept with the user at all times when working off-site. 2.) Locked away in a filing cabinet or drawer when left in the office overnight. 3.) Lock screen must be enabled when not in use.	Mobile computing devices must be: 1.) Kept with the user at all times when working off-site. 2.) Locked away in a filing cabinet or drawer when left in the office overnight. 3.) Lock screen must be enabled when not in use.	Mobile computing devices must be: 1.) Kept with the user at all times when working off-site. 2.) Locked away in a filing cabinet or drawer when left in the office overnight. 3.) Lock screen must be enabled when not in use.
Removable Storage Devices <ul style="list-style-type: none">CDs/DVDsFloppy Disks/TapesExternal Hard DriveUSB Storage Devices	No special precautions required.	No special precautions required.	Removable storage devices must be: 1.) Files must be password-protected in accordance with the <i>DLSMC Password Policy and Guidelines</i> . 2.) Stored in a secure location such as a locked filing cabinet or drawer when not in use.	Removable storage devices must be: 1.) Files must be password-protected in accordance with the <i>DLSMC Password Policy and Guidelines</i> . 2.) Stored in a secure location such as a locked filing cabinet or drawer when not in use.
Physical Security				
Item	Public	Internal	Confidential	Restricted
Photographic, Video & Audio Recording Devices	Stored in a secure and safe location when not in use.	Stored in a secure and safe location when not in use.	Stored in a secure location such as a locked filing cabinet, drawers or a safe when not in use.	Stored in a secure location such as a locked filing cabinet, drawers or a safe when not in use.
Destruction & Disposal of Information				
*** Note: Any decision to dispose of DSLMC Information Assets should be made in accordance with the appropriate Records Retention Policies ***				
Item	Public	Internal	Confidential	Restricted
Paper & Film based information	No special requirements, maybe disposed along with general office waste.	No special requirements, maybe disposed along with general office waste.	Should Confidential Information stored on paper or film material is due for disposal, the material containing the Confidential Information	Should Restricted Information stored on paper or film material is due for disposal, the material containing the Restricted Information must be destroyed and disposed of in a secure manner that protects the

<ul style="list-style-type: none"> Paper records & printed material X-ray film 			<p>must be destroyed and disposed of in a secure manner that protects the confidentiality of the information (ex. shredding – preferably using a cross-cut shredder, pulverized, macerated or by incineration)</p> <p>Where the destruction and disposal of the Confidential Information is outsourced to a third party service provider, the third party service provider must:</p> <ol style="list-style-type: none"> 1.) Sign the DLSMC Non-Disclosure Agreement, and 2.) Provide DLSMC with a Certificate of Destruction. <p>Note: The <i>DLSMC Records Destruction Form</i> must be completed prior to the disposal of information assets.</p>	<p>confidentiality of the information (ex. shredding – preferably using a cross-cut shredder, pulverized, macerated or by incineration)</p> <p>Where the destruction and disposal of the Restricted Information is outsourced to a third party service provider, the third party service provider must:</p> <ol style="list-style-type: none"> 1.) Sign the DLSMC Non-Disclosure Agreement, and 2.) Provide DLSMC with a Certificate of Destruction. <p>Note: The <i>DLSMC Records Destruction Form</i> must be completed prior to the disposal of information assets.</p>
--	--	--	---	--

Destruction & Disposal of Information				
*** Note: Any decision to dispose of DLSMC Information Assets should be made in accordance with the appropriate Records Retention Policies ***				
Item	Public	Internal	Confidential	Restricted
<p>Computing devices</p> <ul style="list-style-type: none"> Laptop Computers Desktop Computers Mobile Computing Devices External/Portable Storage Devices (HDD, USB) 	<p>Must be disposed in accordance with existing environmental laws and regulations and must have a Certificate of Destruction.</p>	<p>Must be disposed in accordance with existing laws and regulations and must have a Certificate of Destruction.</p>	<p>All traces of Confidential Information must be removed from old/obsolete laptop/desktop computers, mobile computing devices, removable storage devices (ex. external hard drives, USB storage devices) before they are reused within DLSMC, sold to staff, donated to charity, or disposed of. The deletion or formatting of Confidential Information stored on the old/obsolete device is not sufficient to remove all traces of information.</p> <ol style="list-style-type: none"> 1.) Where the old/obsolete devices are to be re-used within DLSMC, sold off to employees or donated to charity, the information on the devices must be overwritten using a special Data Wiping software. 2.) Where the old/obsolete devices have come to the end of its working life and are to be disposed of, the devices must be physically destroyed in such a way that it is impossible to recover any Confidential Information stored on the device. <p>All computer devices must be disposed of in accordance with existing environmental laws and regulations and must have a Certificate of Destruction.</p>	<p>Restricted Information should be disposed in the same way as Confidential Information.</p>

Destruction & Disposal of Information				
*** Note: Any decision to dispose of DLSCM Information Assets should be made in accordance with the appropriate Records Retention Policies ***				
Item	Public	Internal	Confidential	Restricted
Photocopiers, Scanners and Fax Machines	Must be disposed in accordance with existing environmental laws and regulations and must have a Certificate of Destruction.	Must be disposed in accordance with existing environmental laws and regulations and must have a Certificate of Destruction.	<p>Most multifunctional photocopiers and scanners contain a Hard Disk Drive which stores a copy of every document that was ever copied, scanned or faxed on the device. For this reason, old and end-of-life photocopiers must have its hard drive physically destroyed to ensure any Confidential Information cannot be recovered from the Hard Disk Drive.</p> <p>All photocopiers, scanners and fax machines must be disposed of in accordance with existing environmental laws and regulations and must have a Certificate of Destruction.</p>	<p>Most multifunctional photocopiers and scanners contain a Hard Disk Drive which stores a copy of every document that was ever copied, scanned or faxed on the device. For this reason, old and end-of-life photocopiers must have its hard drive physically destroyed to ensure any Restricted Information cannot be recovered from the hard drive.</p> <p>All photocopiers, scanners and fax machines must be disposed of in accordance with existing environmental laws and regulations and must have a Certificate of Destruction.</p>

Destruction & Disposal of Information				
*** Note: Any decision to dispose of DLSMC Information Assets should be made in accordance with the appropriate Records Retention Policies ***				
Item	Public	Internal	Confidential	Restricted
CDs & DVDs	No special requirements.	No special requirements.	<p>Old CDs/DVDs that contain Confidential Information must be physically destroyed in such a way that it is impossible to recover any of the Confidential Information stored on the device. For example:</p> <ul style="list-style-type: none">• Shredded using a disc shredder• Cut up with a scissors into small pieces• Using sand paper to destroy both surfaces of the CD/DVD• Incineration	<p>Old CDs/DVDs that contain Restricted Information must be physically destroyed in such a way that it is impossible to recover any of the Restricted Information stored on the device. For example:</p> <ul style="list-style-type: none">• Shredded using a disc shredder• Cut up with a scissors into small pieces• Using sand paper to destroy both surfaces of the CD/DVD• Incineration
Destruction & Disposal of Information				
*** Note: Any decision to dispose of DLSMC Information Assets should be made in accordance with the appropriate Records Retention Policies ***				
Item	Public	Internal	Confidential	Restricted
Floppy Diskettes, Magnetic Tapes (ex. backup tapes)	No special requirements.	No special requirements.	<p>The deletion or formatting of old floppy diskettes and magnetic media is not sufficient to remove all traces of Confidential Information stored on the floppy diskettes or magnetic tapes.</p> <p>Old floppy diskettes and magnetic media that contain Confidential Information must be physically destroyed in such a way that is impossible to recover any Confidential Information stored on the device.</p>	<p>The deletion or formatting of old floppy diskettes and magnetic media is not sufficient to remove all traces of Restricted Information stored on the floppy diskettes or magnetic tapes.</p> <p>Old floppy diskettes and magnetic media that contain Restricted Information must be physically destroyed in such a way that it is impossible to recover any Restricted Information stored on the device.</p>



RECORDS RETENTION AND DISPOSITION SCHEDULE

Records Title and Description	Retention Period	Disposition Authority / Remarks
	Storage	
1. Emergency Case Records/ blotters and other records of prospective medico-legal significance <ul style="list-style-type: none">• Gun Shot Wounds• Mauling of any Nature• Poisoning Cases• Stab/Hacking Wounds• Sudden Death of• Unknown or suspicious cases• Vehicular Accidents	25 years	
2. Certificates <ul style="list-style-type: none">• Birth (not official copy)• Death (not official copy)• Medical	5 years	Retain until patient reaches age of majority (18 yrs) for Birth Certificate
3. Consent to Involvement in Medical Trial		Dispose 1yr. after completion of medical trial. If pre
4. In- Patient Chart Basic Medical Records <ul style="list-style-type: none">• Clinic and Graphic Record/Graphic Chart/TPR Chart•Consent to Hospitalization•Cover sheet/Face sheet/Admission-Discharge Record•Discharge Summary•Laboratory Record•Nurses Notes/Nursing Records•Personal History• Physical Examination•Physicians/Doctors Order Sheet•Progress Records/Progress Notes/ Doctor’s Progress NotesSupplemental Records<ul style="list-style-type: none">• Anti-Coagulant Therapy Record	15 Years	irrespective of its category and classification DLSCMC shall dispose of medical records beyond fifteen yrs. (15 yrs.) Data pertaining to research may be kept more than 15 years., if deem necessary.

<ul style="list-style-type: none"> •Autopsy Report •Blood Transfusion Record •Consultation Report • Diabetic Record • Dialysis Record • Dietary Record/Report • Discharge against Medical Advice • Electrocardiogram (ECG Block) <ol style="list-style-type: none"> 1. Report 2. Tracing • Fluid Intake and Output Chart • Inhalation Therapy Record • Intravenous Fluid Sheet • Medication Board •Delivery Block <ol style="list-style-type: none"> 1.Labor Room Record 2. Newborn Record 3. Pre-natal Record 4. Summary of Parturition •Operation Record <ol style="list-style-type: none"> 1. Anesthesia 2. Informed Consent for Surgery, Anesthesia and other Procedures 3. Operating Room Record 4. Operative Technique 5. Recovery Room Record 6. Tissue/Biopsy Record • Parenteral Fluid Sheet • Pulmonary Laboratory Blood Gas Analysis • Radio Therapy Record • Referral Slip • Rehabilitation Record • Tissue/Organ Donation • Vital Signs Record 		
5. Indexes <ul style="list-style-type: none"> • Disease • Master Patient • Operation • Physician 	May be stored perpetually	
6. Registers <ul style="list-style-type: none"> • Electrocardiogram (ECG) • Family Planning (Sterilization) • Laboratory <ol style="list-style-type: none"> 1. Bacteriology 2. Blood Chemistry 3. Clinical Microscopy 4. Hematology 5. Hispathology 6. Specimens 	PERMANENT PERMANENT	For agency reference. For agency reference. Dispose 2 yrs. After the last entry provided to item is subject of a medico legal case.

6. Live/Still Birth Medical Records Service (Incoming Medical Records from Wards)	PERMANENT	For agency reference.
• Medico- legal • Radiology 1. C-T Scan 2. Ultrasound 3. X-Ray (Routine/Special Procedure)	PERMANENT PERMANENT	For agency reference. For agency reference.
• Surgical Cases	PERMANENT	For agency reference.
7. Medical Records of Employees Working in DLSMC		Dispose 10 yrs after separation/voluntary resignation or retirement.
8. Out- patient Records (Ambulatory Service)		Dispose 10 yrs. After last consultation/visit.
9. Psychiatric Records	25 years	
10. Records of Infants Delivered in a Health Care Facility		Retain until patient reaches the age of majority (18 yrs.)
11. Registers • Admission and Discharges • Birth • Death • Delivery Room • Emergency Room • Labor Room • Operation Room • Out- patient Service/Department • Prescription of Patients (Prohibited Drugs) • Tumor (Special Registry Book)	PERMANENT	For agency reference
12. Reports • Census 1. Daily 2. Monthly	1yr	Dispose 2 yrs. After preparation of annual report. *Irrespective of its category and classification medical records must be disposed if it is beyond fifteen yrs. (15 yrs.)
• Consumption and Inventory of supplies Incident (Nurses and others)	2 years	
13. Notifiable Diseases • Statistical 1. Annual 2. Monthly 3. Semi-Annual	1yr	*Irrespective of its category and classification medical records must be disposed if it is beyond fifteen yrs. (15 yrs.)
14. Results/Reports of Examinations/Procedures/ Tests • ECG Report/Result and Tracing	5 years	

Laboratory 1. Bacteriology 2. Blood Chemistry 3. Clinical Microscopy 4. Histopathology 5. Parasitology		For all laboratory, X-Ray, ECG and other examinations requested as a product of hospitalization/ confinement, the original copy must be incorporated in the medical records. The first duplicate must be maintained by the service concerned as “Official File”. If the result is a product of an OPD Consultation, then the original must be incorporated with the OPD Record.
15. Requests Access to Clinical Information from Medical Records		*Irrespective of its category and classification medical records must be disposed if it is beyond fifteen yrs. (15 yrs.)
ECG		Dispose 1 yr. from date/ release of official report/ result.
Laboratory 1. Bacteriology 2. Blood Chemistry 3. Histopathology 4. Parasitology 5. Urinalysis		Dispose 1 yr. from date/ release of official report/ result
• Release of Information		Attach to Medical Records and follow disposition authority under Item No. 15 Dispose 1 yr. after date of receipt.
Research		Dispose 1 yr. after date of receipt.
X-Ray 1. C-T Scan 2. Routine 3. Special Procedures 4. Ultrasound		Dispose 1 yr. from date/ release of official report/ result.
X-Ray Films • With Court Case		*Irrespective of its category and classification medical records must be disposed if it is beyond fifteen yrs. (15 yrs.)

<ul style="list-style-type: none">• Without Medico-legal Case	10 years	NOTE: X-ray Films of interesting cases with teaching and research significance may be maintained beyond 10 yrs. Depending on the decision of the hospital management.
---	----------	---

Note:

For other personal information and sensitive information processed by DLSMC, the retention and disposal of such data were regarded as industry based and thus indicated in the Privacy Manual under the provisions on Retention.

DATA PROCESSING SYSTEMS INVENTORY

Data Processing System Name	Description
1. Accounts Receivable	This process allows the department/unit to submit billings to patient and patient’s guarantor, and to comply with the requirements to Philhealth.
2. Billing and Collection	This process involves efforts of the hospital to determine patient’s eligibility to its services and assess the capabilities of patients in relation to the medical services availed by the patients.
3. Billing Process	Generation of partial or final bill of patients through printing of Official Statement of Account (SOA) to be provided to patient’s relative for settlement upon discharge. SOA contains personal information of patient such as name, age, address, attending doctor and total charges.
4. In-House Collection	The process involves interview on patient’s relative for admission focusing on source of income of the party responsible to pay for the hospital bill of the patient. The process aims to align the financial capacity of the party responsible for the account versus the projected hospital bill that may be incurred during admission.
5. Patient Admission Process	<p>This process involves the following processing activities</p> <ul style="list-style-type: none">a. Collection of patient data using Personal Information Sheetb. Encoding of patient data in Bizboxc. Printing of Patient Admission Formd. Endorsing Patient Admission Form to Nurse’s Station to be part of the patient’s chart <p>The Scope of this process is from admission of incoming patient/data subjects via Admitting Office, Emergency Room, Delivery Room, Operating Room or from other hospitals via transfer until the time the patient is admitted to their respective rooms as an-inpatient.</p> <p>This process uses tools such as Personal Information Sheet, Patient Admission Form and Bizbox.</p>
6. Philhealth Processing	<p>Checking and evaluation of Philhealth membership.</p> <p>Posting of amounts for deduction based on list of medical & surgical case rate</p> <p>Coding and checking completeness required documents in the system</p> <p>Checking encoded Clinical Chart in e-HR</p> <p>Electronic Filing of Claims in the system</p> <p>Accomplishing Deficiencies of return claims/appealing denied claims.</p>
7. Social Services	<p>In this process the assessment, evaluation, recommendation and approval of potential clinical / PCSO patients seeking medical/financial assistance from the Social Service Section takes place.</p> <p>Collected information will be used to assess socio-economic status of the patient and evaluates if eligible for admission as clinical patient. Once identified, the social worker computes and provides clinical discount upon discharge.</p>
Ancillary (Diagnostic)	
1. CT/MRI	Diagnostic Imaging service which covers the proper collection of data /information from patient undergoing

	<p>diagnostic procedures.</p> <p>This process uses BizBox Hospital Information System v8.0." In this process, patients undergo radiology services in which health data will be recorded in the medical equipment and a hard copy will be released and disclosed to the patient.</p>
2. Blood Bank Donor Screening and HIV Testing	Covers initial screening test for donors. Consent forms are in place before they proceed with the test. Medical data will be collected and results will be generated therefrom.
3. MAMMO & BMD	Signed-off
4. Conventional and fluoroscopy procedure	To provide detailed instructions /guidelines in facilitating fluoroscopy and conventional X-ray procedures
5. Chemistry and Immunology laboratory request	<p>The Clinical Chemistry Section performs a wide variety of quantitative analysis of body fluids.</p> <p>The Immunochemistry Section performs various immunologic assays for the detection and identification of circulating antigens and antibodies in human serum. It utilizes. Electrochemical luminescence assays for the detection of thyroid & fertility hormones, tumor, anemia, bone, and cardiac markers.</p>
6. Routine Clinical Microscopy laboratory request (Urine Analysis)	<p>Personal data is collected as part of a routine medical exam, pregnancy checkup, pre-surgery preparation, or on hospital admission to screen for a variety of disorders, such as diabetes, kidney disease and liver disease.</p> <p>The purpose is to diagnose and monitor medical condition.</p>
7. Routine Hematology laboratory request	<p>This process involves blood testing used to evaluate your overall health and detect a wide range of disorders, including anemia, infection and leukemia.</p> <p>To monitor and diagnose patient medical condition and treatment.</p>
8. Ultrasound	Signed-off
9. Laboratory	Signed-off
Finance	
1. Payroll Process Employees/residents	<p>Creation and computation of DLSCMC employees' compensation and accurate remittance of tax and contributions mandated by law.</p> <p>This process uses the following software tools:</p> <p>1) HR US Personnel Information and Timekeeping System</p> <p>2) Employee Self Service</p>
IT	
1. CF4 Outpatient	Electronic Records of patient for Philhealth Claim. The scope covers maintenance only on the part of the IT Dept.
2. Corporate Website Management	Signed-Off
3. Electronic Health Record	This process involves encoding of patient's data to a soft copy or in the system in compliance with DOH Circular No. 2018-0131 known as the Revised Assessment tools for Hospital and an implementation of the electronic medical records.
4. Electronic Professional Fee Process	Signed-Off
5. Hospital Information System	Involves processing of personal data which starts from encoding of health data to uploading in the system and storage to the database.
6. HRIS	Process which exclusively undertaken by the Information Technology Department which involves system maintenance of the database of the system used by Human Resources Department. They have back-end access to the system.

7. DLSCMC My Results	This is a platform used by patients to access results of their medical examinations. A tool provided to patient to view results over the internet using this link https://myresults.dlsmc.ph using credential provided by laboratory department.
BIOMED	
1. Laboratory Information System (LIS)	LIS is a system for electronic management of laboratory information. It's scope covers from transmitting of data encoded on HIS to LIS to transmitting of information to modality and back to LIS.
2. Picture Archival Communication System (PACS)	PACS is a platform where medical images can be viewed and serve as data storage system for medical images.
3. Radiologic Information System (RIS)	RIS is a system for electronic management of radiology information. It is a networked software system for managing medical imagery and associated data. A RIS is especially useful for tracking radiology imaging orders and billing information, and is used in conjunction with PACS and VNAs to manage image archives, record-keeping and billing. It's scope covers from transmitting of data encoded on HIS to RIS to transmitting of information to modality and back to RIS
4. Medical Imaging	Medical imaging refers to various equipment that are used to view the human body in order to diagnose, monitor, or treat medical conditions. This covers from the receipt of transmitted information from RIS / manual input of information by staff to storage of information on system internal storage.
5. Lab Diagnostic System	Laboratory Diagnostic Systems are medical equipment used to process patient specimens. It processes data based on demographics and information provided by a patient and provides values based on identified computations. This covers from the receipt of transmitted information from LIS / manual input of information by staff to storage of information on system hard drive
6. Therapeutic System/s	Therapeutic system refers to medical equipment that involves treatment of disease and the action of remedial agents. From encoding of data to the machine to equipment storage.
7. Diagnostic System/s	Diagnostic system refers to medical equipment that captures medical vital signs. This includes patient monitors, stress test systems, and the like. It covers the encoding of data to the machine up to their individual storage.
MEDA	
1. Medical Records	This process involves the safekeeping of patient medical records within the retention period allowed by applicable law. The scope of this process is from receipt of data from doctors up to filing of patient's chart, clinical coding and lastly the storage of the patient medical record either in the computer based system or in the manual filing system.
2. Medical Records Department- Releasing and Verification	This process involves releasing/ issuance of medical records to the data subject or its representatives.
3. Bank Enrollment	Personal Data is collected for bank enrollment. Hence disclosure to concerned departments and third-party banks.
4.Complaint Handling	The process which aims to streamline communication and escalation of complaints and incident reports. Incident reports are narrated in an Incident Report Form and is escalated to proper channels.

5. Medical Affairs Database	<p>process of gathering and safekeeping of physician information.</p> <p>The personal information of physicians (PGI, residents and consultants) are collected through an application form. Such documents of the consultant/physicians are scanned and encoded, saved in the local hard drive.</p> <p>Physical documents are placed in envelopes, filed under their respective clinical departments.</p>
6. Recruitment	process which covers recruitment of physicians for training or practice in the institution.
7. Screening and Credentialing	Process which ensures that a fair and unbiased procedure in the process of evaluating competency of a physician to practice his specialty is observed.
Engineering & Maintenance	
1. Sanitary Permit Application	<p>Process involving Sanitary Permit application which is done annually for City Health Department Compliance.</p> <p>The following personal data is collected and disclosed: Names of applicants, Health Certificate application form, Laboratory results, HIV- Aids attendance sheet, photocopy of company ID of authorized person or representative, home address, position, PRC ID. This covers from receipt of data to disclosure with QC health Dept.</p>
Patient Experience	
1. Customer Complaints Management	To properly execute feedback management; analyze and resolve complaints. Complaints are stored in a spreadsheet manner
Ancillary Services (Therapeutic)	
1. Rehabilitation Medicine	Covers the areas of services encompassing the diagnosis and treatment of physical and functional disorders involving the neuromuscular, musculo-skeletal and cardiopulmonary systems. Our department has Physiatrist (Rehab Doctors), Physical Therapist and Occupational Therapist. This process uses BizBox Hospital Information System v8.0.
2. Respiratory Therapy	Focused upon the diagnostic and rehabilitation healthcare needs of patients with respiratory healthcare problems. This process uses BizBox Hospital Information System v8.0.
3. Pharmacy	This involves processing of patient demographic information for documentation. This also includes processing of patient charts and accomplishment of Comprehensive Medication Regimen Form divided into several parts. This process starts from the manual accomplishment of forms up to administering medicines to patients.
5. X-ray	This process involves registration of patient's data to an online platform called Bizbox. Health data that will be captured by the medical equipment will be given to the patient in hard copy form.
6. Heart Station	This process involves various equipment gathering data. This will involve as well releasing of records in a thermal paper print out or DVD. Other personal data will be shared to HMO providers and even technicians of the equipment.
NSO	
1. Fetal Death and Birth Certificate	This process involves collection of personal data of data subject through their representative/s. The personal data shall be recorded in a manual form for the issuance of the birth/death certificate.

2. Ward Care Services – ER, OPD, Nurse Station/s	The processes involve collection of personal data in manual forms to be used either by doctors or nurses attending a patient. Such data will be used to enable personnel to provide quality medical services -
Human Resources	
1. Recruitment	The HR recruitment process is designed to staff the organization with the new employees, and it uses many different recruitment sources to attract the right talent in the defined quality and within a defined time. Uses automatic processing system - Recruitment Management System.
2. 201 File Management	Employee Database
3. Employee Relations	Involves policy compliance, administrative case investigation and employee discipline
4. Benefits, Wages and Administration	The wage and salary administration aims to establish and maintain an equitable wage and salary structure and an equitable labor cost structure and to improve motivation and morale of employees and to improve union management relations. It also pertains to benefits processing of employees and compliance with government mandates and requirements.
5. HRUS	This process aims to provide employees exercise their rights as an employee and as a data subject which include, Leave application, Overtime, Undertime, Official Business, Change of work schedule, attendance adjustments, Loan applications, COE application and salary deduction requests.

DATA PRIVACY PENALTIES FOR VIOLATIONS

The penalties provided herein below shall be construed in a manner consistent with the HR Code of Conduct under the Procedures on Progressive Discipline and subsequent provision on Guidelines.

The following are the corrective measures to be taken when an employee commits any of the violations stipulated in this Code of Conduct.

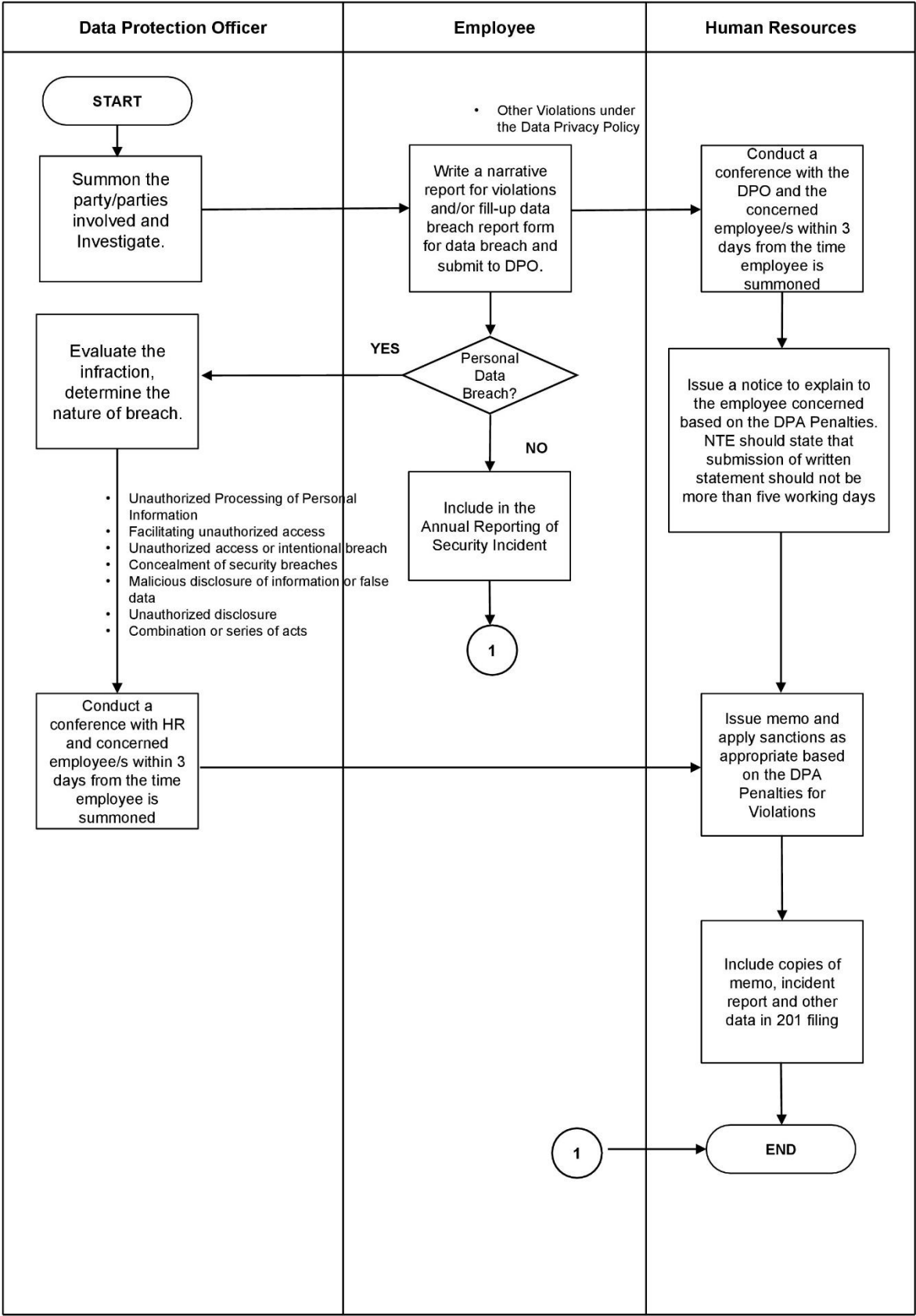
Activity	Steps
Preliminary Actions	<ul style="list-style-type: none">Do a thorough investigation which includes collecting all information and applicable records.
Oral/Verbal Warning (VW) and Final Written Warning (FWW)	<ul style="list-style-type: none">The DPO should have a full discussion with the employee before giving out the warning to ensure that the employee has the opportunity to respond.In cases wherein the IS believes that a verbal warning is appropriate, it should be made clear to the employee that the verbal warning is the first step in the discipline process.The verbal warning must be documented for the Department’s and HRD record.
Written Warning (WW)	<ul style="list-style-type: none">After an employee has received a VW, a subsequent offense should be addressed by a WW as appropriate.DPO must review and draft a written warning in consultation with HRD.DPO and employee meet to discuss the problem. In this discussion, the DPO must review the incident or performance problem which requires a reprimand.The written reprimand should be given to the employee directly following the discussion duly signed by employee with copies to the HRD.
Suspension	<ul style="list-style-type: none">Prior to determining if an employee should be suspended, the DPO must meet with the employee to discuss the seriousness of the problem and consult with HRD.DPO shall prepare a Notice to Explain in consultation with HRD and schedule a meeting with the employee. The NTE must contain all pertinent information.Upon submission of the NTE, DPO must set another meeting to discuss and give the employee his opportunity to explain his side together with HRD and a representative from the Labor Union Officers.Issue a Notice of Decision or Notice of Disciplinary Action implementing the suspension decision.
Dismissal	<ul style="list-style-type: none">DPO shall discuss with HRD the reason and circumstances, past record and any new circumstances leading to the decision of Dismissal.

	<ul style="list-style-type: none">• DPO in consultation with HRD shall prepare a Notice to Explain containing all relevant and pertinent information to the employee.• Once submitted, a meeting should be scheduled with the concerned employee to give him the opportunity to explain his actions together with HRD and a representative from the Labor Union Officers• HRD shall review all records of the disciplinary process and shall submit a recommendation of dismissal or not to terminate to Management.• Once approved, HRD shall issue a Notice of Decision to employee concerned.
--	---

A. Guidelines:

1. For other violations as stated Document any incident report, gather information, review the Data Privacy Manual and Data Privacy Penalties for Violations and determine degree of infraction.
2. In preparing the NTE, it should contain the following and adhere to the Due Process as stated in the Labor Code:
 - a. Details of the incident
 - b. The offense being charged to the employee concerned and its corresponding penalty if proven guilty.
 - c. The submission of the explanation letter which must be **5 working days** upon receipt of the employee.
 - d. Schedule and date of administrative hearing
 - e. The employee’s right to counsel and assistance from the labor union (if the employee is a member of the bargaining unit).
 - f. Consequences for non-compliance and refusal to submit his explanation letter and attend the disciplinary hearing.
3. At the time of commission of the latest infraction, the employee has previously violated other separate rules embraced in the other hospital rules the penalty of which remains unserved, the penalty of the latter infraction is cumulative to the former.
4. The foregoing notwithstanding, it is understood that in cases wherein the offense or infraction was committed in conspiracy or connivance, whether directly or indirectly, with another employee or outside or when the offender, is one wherein the acts or omission committed has the tendency to cause or has caused adverse effect on the good reputation of the institution, the penalty imposed shall be dismissal from employment.

B. Process Flow



C. RESPONSIBILITY AND ACCOUNTABILITY MATRIX

- Discipline is the responsibility of the Immediate Supervisor and Department Head.
- Data Protection Officer must be consulted with regard to policy interpretation, the disciplinary process and procedure and the appropriateness and correctness of the offense cited.
- If the employee becomes aware of any incident or infraction of the Data Privacy Policy, he is to report any violation to the DPO.

4. All disciplinary cases should be resolved within the fifteen (15) working days timeline. Any request for extension on resolving disciplinary cases shall be approved by the President.

Level of Offense	Responsible	Accountable	Consulted	Informed
Verbal & Written Warning	DPO	Department Head	HRD and DPO	Labor Union
Suspension	DPO	Department Head	HRD and DPO	Division Head Labor Union
Dismissal	DPO	Department Head HRD	HRD and DPO	President & CEO Labor Union

Legend:

VW	Verbal Warning	3D	Three Days Suspension
WW	Written Warning	6D	Six Days Suspension
FWW	Final Written Warning	12D	Twelve Days Suspension
1D	1 Day Suspension	D	Dismissal from Service

D. SCHEDULE OF PENALTIES FOR DATA PRIVACY VIOLATIONS

OFFENSES/VIOLATIONS	CORRECTIVE ACTIONS							
	1 ST	2 ND	3 rd	4 th	5 th	6 th	7 th	8 th
1. Unauthorized Processing of Personal Information								
Unauthorized copying, photocopying or reproduction of any manual form containing personal information.	FWW	3D	6D	12D	D			
Unauthorized recording and capturing of any personal information through any media recording device not sanctioned by the company.	FWW	3D	6D	12D	D			
Uploading, posting and sharing personal information of the company’s data subject in any social media platform not authorized by the company and without the consent of the data subject.	3D	6D	12D	D				
Willful dissemination of any personal information belonging to the company’s	3D	6D	12D	D				

data subject to other employee or any person outside the company.								
Failure to secure the consent of a data subject prior to any processing activity in accordance with the data privacy policy of the company	FWW	3D	6D	12D	D			
Willful, repeated and deliberate use of manual forms containing personal information as scrap paper or scratch paper.	FWW	3D	6D	12D	D			
Any of the violation/s stated above involving sensitive personal information where there is gross negligence, malice, ill-will or bad faith shall have the following corrective action.	D							
2. Facilitating unauthorized access								
Allowing any person not authorized to access or have access to personal data pertaining to any company's data subject.	FWW	3D	6D	12D	D			
Failure to apply reasonable security measures implemented by the company to protect the personal information of its data subject from unauthorized access.	FWW	3D	6D	12D	D			
Sharing of email account information and account passwords to any person not authorized to access personal information processed therein.	FWW	3D	6D	12D	D			
Any of the violation/s stated above involving sensitive personal information where there is gross negligence, malice, ill-will or bad faith shall have the following corrective action.	D							
3. Unauthorized Processing of Personal Information								


Disposal of personal information within the retention period imposed by the company.	WW	FW W	3D	6D	12D	D		
Disposal of manual forms containing personal information not in accordance with the disposal policy.	WW	FW W	3D	6D	12D	D		
Intentional or accidental deletion of personal information of data subject causing availability breach.	12D	D						
Any of the violation/s stated above involving sensitive personal information where there is gross negligence, malice, ill-will or bad faith shall have the following corrective action.	D							
4. Unauthorized access or intentional breach								
Unauthorized bringing of documents outside the company premises containing personal information.	FWW	12D	D					
Use of personal email containing personal information of company's data subject.	FWW	12D	D					
Performing any act to compromise a computer system, software, program or any IT system which causes an actual confidentiality, integrity and availability breach.	D							
Unauthorized use of email account or any account information to access file containing personal information which causes confidentiality, integrity and availability breach.	D							
Any of the violation/s stated above involving sensitive personal information where there is gross negligence, malice, ill-will or bad faith shall have the following corrective action.	D							

5. Concealment of security breaches								
Failure to report security incident / personal data breach within 24 hours from knowledge or upon reasonable belief that a security incident occurred.	FWW	12D	D					
Having knowledge of the identity of the person who committed any of the data privacy violation and willfully decide not to report the breach and person who caused it within 24 hours from knowledge.	FWW	12D	D					
Concealing, tampering or destroying the body or any evidence of breach, or the effects or instruments thereof, in order to prevent its discovery.	12D	D						
Prolonging the course of the investigation with the intention to conceal the discovery of security incident or personal data breach.	D							
Causing unnecessary delay which subjects the company from violating the 72-hour notification requirement of breach to the NPC.	D							
6. Malicious disclosure of information or false data								
Disclosure of data which may cause injury or damage or which may create real risk or harm to the company's data subject.	6D	12D	D					
Willful and intentional disclosure of any malicious information pertaining to a data subject other than rumor mongering which causes injury or damage to the data subject or that of its representative, guardian or ward.	6D	12D	D					
7. Unauthorized disclosure								

Disclosure of personal information in violation of the company's data privacy manual.	FWW	12D	D					
Disclosure of personal information not in a manner sanctioned by the company.	FWW	12D	D					
Disclosure of personal information to a third-party or to any entity without the consent from the data subject.	6D	12D	D					
Failure to validate the identity of the recipient of personal data upon disclosure or release of medical records or any act of disclosure to person not authorized by the data subject.	3D	6D	12D	D				
Any of the violation/s stated above involving sensitive personal information where there is gross negligence, malice, ill-will or bad faith shall have the following corrective action.	D							
8. Other Violations under the Data Privacy Policy								
Violation of data subject rights or failure to address the request of data subject thereby causing delay without reasonable grounds.	FWW	3D	6D	12D	D			
Failure to exercise due diligence in the collection of accurate personal information from the data subject.	FWW	3D	6D	12D	D			
Processing incorrect, inaccurate and obsolete data from data subjects.	FWW	3D	6D	12D	D			
Due disregard of the existing company policy regarding processing of confidential and restricted data which causes compromise of such information that may or may not cause injury or damage to a data subject.	FWW	3D	6D	12D	D			
Posting and uploading onto any social media platform of	FWW	3D	6D	12D	D			

any file format any personal information of patients and employees including any confidential, restricted and internal data pertaining to a person or the company without consent or authorization from the concerned parties.								
Performing any act which remove, destroy and detach any privacy notice/s in the company premises and privacy clauses and waiver clauses in any document.	FWW	3D	6D	12D	D			
Unreasonable disregard of implementing appropriate physical and technical security measures in the processing system.	FWW	3D	6D	12D	D			
Revealing private employee information to other employers without the employee's consent.	FWW	3D	6D	12D	D			
Releasing unauthorized health information - This refers to releasing the wrong document that has not been approved for release.	FWW	3D	6D	12D	D			
Releasing information about minors without the consent of a parent or guardian.	VW	FW W	6D	12D	D			
Concealment of lost or stolen devices issued by the company.	VW	FW W	6D	12D	D			
Discussing private health information in public areas of the hospital, including the lobby of a hospital, an elevator or the cafeteria.	VW	FW W	6D	12D	D			
Insider snooping - This refers to family members or co-workers looking into a person's medical records without authorization.	VW	FW W	6D	12D	D			
Any and all act or omission that may be deemed as to cause damage to the company and acts which may cause	VW	FW W	6D	12D	D			

harm and risk to its data subject identified by the Data Protection Officer.								
Failure to perform an obligation or performance of any act which violates any obligation or responsibilities indicated in the Confidentiality Undertaking not mentioned in this document.	FWW	6D	12D					
Inciting any authorized person to perform an act which violates existing policies on data privacy and in the confidentiality undertaking.	D							
Unauthorized accessing/ processing of Patient Health Information from Unsecured Location.	D							
Willful and deliberate intent to injure the company or its reputation, any of its affiliates, officers and employees by spreading malicious information that causes injury or damage to the aforementioned personnel.	D							
Failure to adhere to the authorization expiration date – release of patient health information beyond the expiration date of the authorization letter.	D							
Releasing wrong patient information or through a careless mistake, patient information is released to the wrong patient.	D							
9. Combination of series of acts								
Performing combination of any of the acts mentioned above where the penalty prescribed is progressive shall constitute the following corrective actions.	D							
Notwithstanding the table of sanctions and offenses in this handbook, the company reserves the right to impose heavier penalties including dismissal from employment when warranted by the circumstances.								

 De Los Santos Medical Center	NOTICE TO EXPLAIN AND ADMINISTRATIVE HEARING
Employee Name:	Date:
Position:	Department:
I. Details of the Incident	
II. Violation based on the Data Privacy Penalties for Violations/COC and corresponding penalty	
<p>You are hereby given five (5) working days to explain in writing why you should not be meted with administrative sanctions. You are also advised that an administrative hearing will follow on _____ at _____ AM/PM at the _____ of the company.</p> <p>Furthermore, you are free to be represented and assisted by an officer of the labor union during the administrative proceedings. If you fail to appear for the administrative hearing or adduce evidence in your behalf or fail to submit your letter of explanation within the time period indicated shall be deemed a waiver of your right to be heard and to defend yourself, in that event, management shall be compelled to render its decision on the basis of available evidence.</p>	
For your strict compliance	
Immediate Head	Department Head
Date:	Date:
Employee:	Date:

Disclaimer

This Privacy Manual is a property of De Los Santos Medical Center. This material may not be reproduced or distributed, in whole or in part, without the prior written permission of the company except for legitimate purposes or in the exercise of a right as a data subject under the Data Privacy Act of 2012. Any other reproduction or distribution, in whatever form and by whatever media, is expressly prohibited without the prior written consent of the company.

For further information, please contact privacy@dlsmc.ph. All rights reserved.