

DLSMC PRIVACY POLICY

Hi! We are De Los Santos Medical Center.

OUR ROLE IN YOUR PRIVACY

If you are a client or patient of **De Los Santos Medical Center (DLSMC)**, this policy applies to you. It is only natural to want assurance that your data will be in safe hands. We consider your privacy extremely important; through this policy, we will explain which of your data we process and how we handle these data.

OUR RESPONSIBILITIES

We act as the “[personal information controller](#)” of your personal data processed for the provision of healthcare and healthcare services.

Our Data Protection Officer is Atty. Eunice Saavedra. You may reach him via privacy@dlsmc.ph

We also act as the personal information controller for research-related processing of patient data, subject to strict safeguards and ethical oversight.

YOUR RESPONSIBILITIES

- Read this Privacy Policy
- If you provide us with personal information about other people, or if others give us your information, we will only use that information for the specific reason for which it was provided to us. By submitting the information, you confirm that you have the right to authorize us to process it on your behalf in accordance with this Privacy Policy.

TYPES OF DATA WE COLLECT

Data that identifies you

- Your name, age and birthdate, marital status, PhilHealth number, SSS or GSIS number, the details of your valid government identification card, etc.

Health, biometric, biological, and medical information

- Your height, weight, blood type, current symptoms, medical history (including family medical history), information about your lifestyle (e.g., consumption of alcohol or tobacco products), vital signs (temperature, blood pressure, heart rate, etc.), diagnostic information, treatment information (details of surgeries, medications prescribed, doses, administration times, and other treatments). If you have been admitted to the hospital we will also collect information on your medical condition and changes in your condition, treatment responses and outcomes, discharge status, and follow-up care instructions.

Financial Information

- Credit/debit card details, details of your employer, etc.

Contact details

- Your contact number, email address, and home address, as well as the contact details of your next of kin or emergency contact

Other sensitive personal information that may affect our delivery of healthcare services or that we may collect when you access public areas within our premises

- Your religion, race and ethnic origin, CCTV footage (please refer to our separate CCTV Surveillance Notice)

HOW WE USE YOUR DATA

We process data about all patients at our hospital. By 'process', we mean, for example, that we will save or add to your data, or that we will share them with your healthcare providers (e.g., your physicians), and delete them at a later date. If you receive treatment at our hospital, we will process your health and medical information in your patient record. Under no circumstances will we process more data than needed to provide you with the appropriate care.

- **To provide you with medical care**

Legal basis: Necessary for medical treatment, Necessary for the protection of life and health

Your personal information helps us understand your health history and current health needs to provide you with appropriate medical treatment and services. This includes everything from diagnosing your condition to planning your care and treatment. Your information may be used and accessed by our employees and medical consultants (*i.e.*, *your physicians or the healthcare professionals involved in the interpretation of your test results*) who are involved in or who have a supporting role in your care and treatment to ensure that you receive the best possible care. These employees and consultants have a statutory duty and/or ethical and professional duties of confidentiality.

We may share your information with other affiliated clinics or hospitals if you are referred to them. But, we will only share your information after you have consented to it.

- **To communicate with you**

Legal basis: Necessary for medical treatment, Necessary for the protection of life and health

We may use your contact information to communicate important information about your appointments, test results, and health status.

- **For billing and payments**

Legal basis: Necessary for medical treatment, necessary for compliance with a legal obligation

We will process your relevant financial information (such as your credit card information or other information relevant to your mode of payment), insurance or HMO details, and PhilHealth details to ensure that you are properly billed, that your health insurance benefits under PhilHealth and your insurance or HMO are deducted from your bills, and for the payment and settlement of your bills.

- **To comply with legal requirements**

Legal basis: Necessary for compliance with a legal obligation

We are required under various regulations to share health information to the Department of Health, PhilHealth, etc. For instance, we are required to report to the DOH selected non-communicable diseases, communicable, infectious and other notifiable diseases, including those that pose a serious health and security threat to the public. We are also required to share information on your diagnosis and treatment to the PhilHealth to accord you the benefits that may be due to you under the National Health Insurance.

- **To coordinate your care with your healthcare professionals**

Legal basis: Necessary for medical treatment, Necessary for the protection of life and health

Your medical doctors practice in our institution as consultants. Therefore, they are considered as third parties with whom we must necessarily share your information to provide the medical care you need.

- **To send you marketing messages**

Legal basis: Legitimate Interest

We may send you messages to provide health education content, information about our hospital and the services we offer, information and tools that may help you make informed decisions about your health, feedback forms to assess the quality of our services, etc. Nonetheless, we will only send such messages with your prior consent, unless otherwise allowed under applicable laws.

- **To improve our operations and services**

Legal basis: Legitimate interest, vitally important interest, and necessary for purposes of medical treatment

We will process your personal information to standardize your information in the hospital, allowing us, ultimately to improve our operations and services. By standardizing your information, we mean that we will reformat and re-organize your information (including those that we are already keeping) so that your information will follow a standardized format thereby allowing us to clean up our records and enhancing patient safety and coordination of care.

We will process your name (First, Middle, and Last), date of birth, address, gender, information on your government-issued ID (e.g., PhilHealth number), and phone number to unify our records and create a unique patient ID for each of our patients. This will help us understand our patients' care lifecycle and improve patient safety by ensuring that our healthcare professionals have the latest information available to make informed treatment decisions. The unique patient ID will be the hospital's foundation for unifying its disparate patient records and for cleaning up and updating its patients' records.

- **Use of Patient Data for Research**

We may process patient data for scientific and research purposes only under strict safeguards, in compliance with the Data Privacy Act (DPA), NPC Advisory Opinion 2018-54, and the National Ethical Guidelines for Research Involving Human Participants (NEGRIHP, 2022).

Researchers will only be granted access to de-identified or anonymized data unless the use of personal identifiers is essential, justified, and approved by the Research Ethics Committee (REC), or unless consented by the data subject as required by law.

Access to identifiable information (such as names) is prohibited by default and will only be allowed under documented ethics clearance and institutional approval.

All research requests must undergo ethics review and approval prior to data release.

Technical and administrative safeguards, including role-based access controls, audit trails, and secure analysis environments, will be implemented to ensure that researchers access only the minimum data necessary for their approved study.

- **Other uses that are exempt from the coverage of the Data Privacy Act**

In the interest of full transparency, we also use your information for purposes that are exempt from the Data Privacy Act:

- For scientific and research studies,
- For teaching and training our future doctors-specialist, healthcare professionals, and students in the medical and other healthcare fields, and
- For purposes of our business operations and financial performance reporting, statistical analysis, etc.

In all of these cases, we will anonymize or aggregate your information. Otherwise, we will seek your consent prior to using or sharing your information for the above purposes. These activities are conducted in accordance with Section 4 of the Data Privacy Act of 2012, and we ensure that appropriate safeguards, including data minimization and security measures, are in place even when exemptions apply.

For research or teaching use of patient data, DLSMC implements additional safeguards aligned with NPC Advisory Opinion 2018-54 and NEGRIHP (2022), including de-identification, ethics review, and strict access controls described below.

WHEN AND HOW WE COLLECT YOUR DATA

Here's when and how we collect data:

DATA
YOU
GIVE

DATA WE
COLLECT



Through Admitting Section & Outpatient Registration

Upon your arrival at the hospital for admission or surgery your detailed personal and medical information will be collected by our Admissions Department. If you are referred to admissions by our Emergency Department, the information necessary for your admission may have already been collected at the Emergency Department.

- ✓ ✓ If admitted, in the course of your care, through our in-patient services If you are admitted for treatment in our institution, our staff will collect and use your information (such as your diagnostic information, medical condition, dietary information, medication, etc.) for your medical care.
- ✓ ✓ In an emergency, through the Emergency Department In emergency situations, the Emergency Department, and the Triage will quickly collect your information (such as your brief medical history, reason for the visit, and insurance information if readily available) to render timely and adequate medical care.
- ✓ ✓ When you avail of any of our out-patient services, through the department laboratory diagnostic services, etc.) When you avail of our various out-patient services (such as imaging, diagnostics, consultations in our out-patient or primary care centers), we (e.g., collect and/or update your information to reflect services, any changes since your last visit. For laboratory, imaging diagnostics, and imaging, we verify and collect your information to ensure that the tests and the results are accurately matched and recorded to the right patient.

RESEARCH USE OF PATIENT DATA AND ACCESS CONTROLS

In line with the Data Privacy Act of 2012, NPC Advisory Opinion 2018-54, and the National Ethical Guidelines for Research Involving Human Participants (NEGRIHP, 2022), DLSMC permits the use of patient data for research only under strict conditions designed to protect patient privacy and confidentiality.

1) Scope of Access

- Researchers (including PGIs, residents, fellows, clinicians, and students) will, by default, be granted access only to de-identified or anonymized datasets, or to complete set if consented by the Data Subject as required by law.
- Access to personal identifiers (e.g., names, full address, government IDs) is prohibited unless essential to the approved protocol, accompanied by a documented justification, and specifically authorized by the Research Ethics Committee (REC) and the designated Data Controller.
- Only the minimum data necessary for the approved study objectives will be provided (data minimization).

2) Designated Data Controller and Custodians

- DLSMC designates a centralized Data Controller for research-related access to medical records, overseen by the Medical Records Department (in coordination with the Health Information Management and the Data Protection Office).
- Each clinical department will appoint a Data Custodian to support implementation, verify study relevance, and coordinate with the Data Controller on approvals.

3) Request and Approval Process

- Before any access is granted, researchers must submit a formal request that includes: the study protocol, REC ethics clearance (or documented waiver of consent where applicable under NEGRIHP), a variable list, data minimization rationale, and a data retention/destruction plan.
- The Data Controller will review requests for compliance with DPA, NPC advisories, NEGRIHP, and institutional standards, and will approve only time-bound, scope-limited access.

4) Technical and Administrative Safeguards

- Role-based access controls (RBAC) and unique research accounts; no use of personal clinical credentials for research access.
- Audit trails for all data viewing, extraction, transformation, and exports.
- Secure analysis environments (e.g., controlled workstations or virtual research environments) with restricted export of raw records; downloading identifiable data to personal devices or external media is prohibited.
- Mandatory Data Use Agreements (DUAs) covering permitted uses, onward sharing prohibitions, publication rules, and breach notification.
- Data minimization and de-identification by default; re-identification is prohibited unless expressly approved and technically justified.
- Time-bound access with automatic revocation and documented data destruction/archiving at study end.

5) Consent, Ethics, and Legal Bases

- Research involving patient data will follow NEGRIHP (2022) requirements for informed consent or ethics-approved waivers, confidentiality, and risk minimization.
- Where the DPA research exemption (Section 4[e]) applies, DLSMC will still implement appropriate safeguards, including de-identification, access controls, and ethics oversight consistent with NPC Advisory Opinion 2018-54.

- Research data will never be used to make decisions about an individual's care unless integrated into the medical record under appropriate clinical and legal bases.

6) Accountability and Sanctions

- Violations of this section or the DUA may result in revocation of access, administrative or disciplinary action, reporting to the REC, and notification to the National Privacy Commission where required.

For more details, please refer to our institutional Data Access Policy for Research and REC Standard Operating Procedures.

YOUR PRIVACY RIGHTS AND CHOICES

You have the right to access the information we hold about you

This includes the right to inquire upon:

- The contents of your personal information that we process,
- Where we obtained your personal information,
- Names and addresses of those who received your personal information,
- Manner by which we process or processed your personal information,
- Any automated process we employ where your data will or likely be made as the sole basis for decisions affecting, or that may affect, you, etc.

For more information on the matters for which you may demand access, please refer to the Data Privacy Act of 2012 and its implementing rules.

You have the right to make us correct any inaccurate information about you

You have the right to lodge a complaint regarding our use of your data

Please tell us first, so we have a chance to address your concerns. If we fail to do this, you may lodge your complaint with the National Privacy Commission.

Please note that you have other rights under the Data Privacy Act of 2012, in addition to those which we have listed in this Notice.

Specifically, you also have the right to object to the processing of your data, to request the erasure or blocking of your data under certain circumstances, and to data portability. For more information, please refer to Section 16 of the Data Privacy Act of 2012.

THIRD PARTIES WHO PROCESS YOUR DATA

We use third parties to provide and deliver our healthcare services to you. Because of this, it is necessary for us to share your data with these third parties. Your data is shared only when strictly necessary and where there are safeguards. If your data needs to be transferred to a third-party in another country, we will conduct a risk assessment to ensure that there is an adequate level of protection. We will only proceed with such

transfers if the receiving country is deemed to have adequate data protection standards, or if appropriate safeguards (such as model contractual clauses) are in place, in accordance with NPC Advisory No. 2024-01. We will usually include these obligations in our contracts with said third parties. In addition, all data transfers whether within or outside of the Philippines are encrypted. Below are the third-parties who help us process your data:

Health and Medical Services

Third Party	Data Collected or Shared	Purpose	Place of Processing
Medical Consultants	Personal identifiers of patients and their medical and clinical information	To provide medical care and coordinate your medical care with your healthcare professionals	Philippines
Academic and Research Collaborators (when applicable)	Only anonymized or de-identified datasets, or limited variables approved by the REC and the Data Controller, or unless consented by the Data Subject as required by law.	Conduct of ethically approved research under DUA and strict safeguards	Philippines

Payments

Third Party	Data Collected or Shared	Purpose	Place of Processing
PhilHealth	Full Name, Period of Confinement, Patient Disposition, Type of Accommodation (if in-patient), Admission Diagnosis, Discharge Diagnosis, and Treatment Information	For the reimbursement of claims pursuant to the National Health Insurance Act and its implementing regulations.	Philippines
HMOs (You may request the list of our accredited HMOs from our Admissions Department)	Full Name, Employer, Age, HMO account number, and Diagnosis	To process your claims against your insurance provider.	Philippines

or you may view the list in our website)			
Payment Partners (Maya, Gcash, Bank POS Terminals)	For Maya and Gcash: Transaction Type, Batch Number, Reference Number, Approval Code, Date and Time of Transaction, Network Reference Number, and Amount Bank POS Terminals: Credit or Debit Card Information, Amount, and Cardholder Signature	To process and verify the payment of your bills.	Philippines

HOW WE SECURE THE DATA WE COLLECT

We use administrative, technical, organizational, and physical security measures that are designed to protect your personal information from unauthorized access, use, alteration, and disclosure. We also take steps to ensure that third parties that have access to your personal information take steps to protect the same. However, please remember that:

- No data transmission is guaranteed to be 100% secure.
- If you believe your privacy has been breached, please contact us immediately through our Data Protection Officer.

Moreover, in line with the Data Privacy Act of 2012, NPC Advisory Opinion 2018-54, and the National Ethical Guidelines for Research Involving Human Participants (NEGRIHP, 2022), we allow the use of patient data for research only under strict conditions:

- Researchers must secure ethics clearance from the Research Ethics Committee (REC) and submit a formal request to the designated Data Controller.
- Only the minimum necessary data elements approved by the REC will be provided. Personal identifiers (such as names) are prohibited unless explicitly justified and approved.
- Technical and administrative safeguards will be applied, including role-based access controls, audit logs, secure analysis environments, and mandatory Data Use Agreements.
- Violations of these safeguards will result in sanctions, including revocation of access and reporting to the ethics committee.

WHERE DO WE STORE YOUR DATA

We store physical copies of your data in our Medical Records Department. We also store electronic copies of your information in our Hospital Information System (HIS) that has an on-site server.

HOW LONG DO WE STORE YOUR DATA

We will retain your information for as long as necessary to serve the purposes for which they were obtained. Please know, however, that the periods for the retention of medical records are likewise governed by Philippine laws, rules, and regulations, including DOH Department Circular No. 70-1996 (which provides for the retention period of various health records), DOH Department Circular No. 2021-0226, and DOH Administrative Order No. 2022-007 (which provides for retention periods of documents, records, slides and specimens in clinical laboratories). We will, therefore, also retain your information for as long as necessary to comply with our obligations under said laws, rules, and regulations.

CHANGES TO THIS NOTICE

We may change or update our Notice to comply with regulatory requirements, adapt to new protocols, align with industry practices, and for other legitimate purposes. We will let you know should we implement any such changes at the earliest opportunity. If necessary, we will also obtain your updated consent.

OWNERSHIP	CHANGE	NOTIFICATION
In the event of a change in ownership of DLSMC, we remain committed to maintaining privacy and security of your personal data. We will notify affected data subjects if their data has been compromised due to transfer of ownership. This communication will be made to inform data subjects of any potential impacts on their personal information and the measures being taken to ensure data protection.		

What do these legal bases mean?

NECESSARY FOR MEDICAL TREATMENT

We may process your data without your consent if the processing is necessary for us to provide adequate treatment. Necessary means that the processing is not only merely desirable but is essential to the provision of medical treatment. Under this legal basis, we will only process your information to the extent reasonable and using or processing only the data needed to provide said medical treatment.

NECESSARY FOR THE PROTECTION OF LIFE AND HEALTH

We may process your data without your consent if it is necessary for the protection of your or a third person's life or health but you or the third person are physically or legally unable to provide consent. We will only process your information to the extent reasonable and using or processing only the data needed for the protection of your or a third-person's life and health.

LEGITIMATE INTEREST

As an organization, we may process your data to carry out tasks related to our operations and business activities. These legitimate interests include:

- Getting insights on the needs of our clients and patients to improve clinical care, patient safety, service offerings, and the quality of our services.
- Understanding trends, managing our resources better, and improving our treatment protocols.
- Preventing fraud and ensuring that our network and information systems are secure.



LAW

In specific instances, we may process your data without your consent, if such processing is required by law and regulations, if said regulations guarantee the protection of the information and do not require the consent of the data subjects. We will only process your information to the extent reasonable and only for purposes of fulfilling the relevant legal or regulatory requirements.

CONSENT

You have given us clear consent to use and process your data for a specific purpose.

You can change your mind!

If you have previously given your consent to our processing your data you can freely withdraw it at any time by notifying us at privacy@dlsmc.ph. If you do withdraw your consent, and if we do not have another legal basis for processing your information, then we will stop processing your personal data. If we do have another legal basis for processing your information, then we may continue to do so subject to your rights. Please note that it may take up to fifteen (15) business days for us to process the withdrawal of your consent.