Insular Health Care Privacy Statement

We at **Insular Health Care, Inc. ("iCare")** continue in the pioneering spirit of our parent company, Insular Life Assurance Company, Ltd. ("InLife"), the first and largest Filipino life insurance company with an unbroken service record of more than a hundred years. Like our parent company, Insular Health Care has an unbroken service record which now spans almost three decades.

Acknowledging that our continued success largely depends on our reputation, our company is conscientious in adhering with laws and applicable rules and regulations of the industry.

We are bound by, and shall dutifully comply with, **Republic Act No. 10173** or the **Data Privacy Act of 2012 ("DPA")** and its Implementing Rules and Regulations ("IRR"), generally accepted principles of international law on data privacy, and other applicable laws as well as rules and regulations which *require* or *affect* our collection and processing of personal data. These include issuances by the National Privacy Commission ("NPC"), the Insurance Commission ("IC"), the Anti-Money Laundering Council ("AMLC"), the Securities and Exchange Commission ("SEC"), the Bureau of Internal Revenue ("BIR"), and the Department of Labor and Employment ("DOLE").

Concomitantly, we are committed to protecting your privacy as our client, agent, employee, supplier, partner, or even as a visitor to this website. Toward this end, this Privacy Policy will discuss and/or explain the following:

**I. General Information**

**II. Processing of personal data on our website**



**I. General Information**

**Commonly used data privacy terms** As used in the DPA and in this Privacy Policy, the following terms shall have the respective meanings hereinafter set forth:

- **Consent** – refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of personal information relating to him or her. Consent 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. (Sec. 3b, DPA)
- **Data subject** – refers to you, an individual whose personal information is processed. (Sec. 3c, DPA)
- **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. (Sec. 3g, DPA)
- **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 (Sec. 3h, DPA). For purposes of this Privacy Policy, Insular Health Care is the PIC.
- **Processing** – refers to any operation or any 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. (Sec. 3j, DPA)
- **Privileged information** – refers to any and all forms of data which under the Rules of Court and other pertinent laws constitute privileged communication. These include communications learned in confidence between husband and wife, lawyer-client, doctor-patient, and priest-confessor. (Sec. 3k, DPA in relation to Rule 130, Sec. 24 of the Rules of Court)
- **Sensitive personal information** – refers to personal information: (1) about an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations; (2) about an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings; (3) issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or

revocation, and tax returns; and (4) specifically established by an executive order or an act of Congress to be kept classified. (Sec. 3l, DPA)

**Who are we?**

We are **Insular Health Care, Inc.** ("iCare"), a corporation duly organized and existing under the laws of the Republic of the Philippines, and duly licensed by the Insurance Commission ("IC") to engage in business as a Health Maintenance Organization ("HMO"). As an IC Regulated Entity ("ICRE"), we are also an Anti-Money Laundering Act ("AMLA") covered institution. For purposes of this Privacy Policy, we are the PIC which controls the collection, holding, processing and/or use of your personal, privileged, and sensitive personal information.

To know more about our company, including our directors and officers, click here.

**What do we do?**

As an HMO, we set-up, establish, coordinate, offer, provide or otherwise make available a comprehensive and integrated medical and preventive health care services and facilities systems including maternity care, well-baby care, pre-employment medical check-up, industrial clinical services and such other related services to individuals, group of individuals, associations, firms and other organizations. We also conduct studies as to the nature, cause, prevention and treatment of diseases, and disseminate information respecting the same.

**What data do we collect?**

As part of our dealings with you, we collect the following personal, privileged, and sensitive personal information (collectively referred to as "personal data"):

- As mandated by IC and AMLC: your personal information including your full name, sex, date and place of birth, citizenship, civil status, permanent address, present address, telephone and mobile numbers, tax identification number and other government-issued identification numbers, source of funds, specimen signatures or biometric information, identification document or information, and other similar information. (Rule 18 – Customer Due Diligence, IRR of AMLA);

- As mandated by IC and AMLC: your business or employment information, e.g. occupation, rank, name of employer or business, work address and telephone number; (Rule 18 – Customer Due Diligence, IRR of AMLA);
- As mandated by IC and AMLC, information regarding your company including your ownership and/or participation when you apply for vendor, supplier or contractor accreditation. (Rule 16, IRR of AMLA);
- For job applicants, directors, officers, employees and agents: your employment history and records including your social security numbers, educational attainment, *résumé*, income information, and other similar information. (Rule 16, IRR of AMLA; IC Circular Letter No. 2016-51);
- For medical partners and/or employees with professional licenses: your professional information including your field of specialization and sub-specialization, professional affiliations, licenses and other similar information;
- Your medical history, records and information, medication, genetic or sexual life and other information relevant or connected with your HMO coverage from, or of your diagnosis, treatment or availment of health care services at or through Insular Health Care;
- Your social media behavior when you tag, mention, or post photographs relating to Insular Health Care on any social media account, e.g. Facebook, Twitter, Instagram, LinkedIn, etc.;
- Your payment details, e.g. credit card and/or other banking information;
- Information about your visit and use of our websites, digital platforms, and mobile apps, including your social media profile information, IP addresses, your browsing behavior within and throughout our digital assets, and session lengths that are collected by our website analytics tools and cookies that we may place on your computer. You can disable the use of cookies on your browser at any time. (See: “Cookies”, “How do we use cookies?”, “What types of cookies do we use?”, “How to manage your cookies?” and “Additional data collection activities (automated access)”);
- Any information which you choose to share or send to us;
- Any other information relating to you which you have provided us, in submission of any form and/or as a result of our interaction with you either online or offline, in the course of our fulfilment of our legal and/or contractual obligations to you. For this purpose, any availment of health care services or any interaction with any of our

accredited hospitals, clinics, doctors, dentists and medical partners through your HMO coverage with us, shall be deemed as interaction that will result in data collection.

**How do we collect your data?**

We collect your data through personal collection or through mail, phone or online services, depending on "what data we collect", "when we collect your data" and "why we collect your data".

**When do we collect your data?**

You directly provide us with most of the personal data we collect. We collect and process personal data when:

You submit information through manual forms including application forms and personal information sheets, and online forms on our digital assets, i.e. websites, digital apps, or contact us through any of our social media accounts, e.g. Facebook, Twitter, Instagram, LinkedIn, etc.;

- You purchase or avail any of our products and services. (See: "what do we do?");
- You avail of health care services or otherwise interact with any of our accredited hospitals, clinics, doctors, dentists and medical partners through your HMO coverage with us;
- You submit a job application or otherwise become our director, officer or employee;
- You participate in any of our promos, activities, events and sales initiatives;
- You interact with our sales or customer care specialists or agents through email, phone, chat services or face-to-face meetings;
- You visit our premises with CCTV surveillance cameras that are used for safety and security of our guests, employees and visitors;
- You subscribe to our email and/or sms notifications, updates and/or newsletters;
- You provide personal information in relation to inquiries, requests, and complaints;
- You submit your personal information to us for any other reason.

We also indirectly receive your personal data from the following sources:

- Affiliates, related entities and business partners (when you have consented to cross-selling and cross-marketing);
- Vendors, suppliers and contractors that we engaged to help us carry out our legal and/or contractual obligations to you when they have collected your personal data under conditions similar to our data collection and processing. (See: “what data do we collect?”, “when do we collect your data?” and “why do we collect your data?”;
- Building administrators of our offices;
- Security firms engaged to guard our offices.

**Why do we collect your data?**

**1. Uses of your personal data** – We collect your personal data so that we can:

- Properly administer our services including processing claims, underwriting, issuance of letters of approvals and other similar services. (See: “what do we do?”)
- Send you official communications;
- Send you email notifications and/or newsletters, if you have opted for them. You can opt out any time by simply unsubscribing;
- Send you marketing communications relating to our business (or the business of any of our affiliates, related entities and business partners) which we think may be of interest to you, by post or, when you have specifically agreed to it, by email or similar technology.
- Deal with inquiries and complaints made by or about you relating to our products and services;
- Keep our offices, facilities, websites and other systems secure;

- Verify compliance with the terms and conditions governing the use of our websites including monitoring private messages sent through our website private messaging service;
- Comply with legal requirements as well as legal proceedings and processes such as court orders, and prevent imminent harm to the public. (See: "when  are we obliged to disclose your data even without your consent?");
- Prevent, detect and investigate crimes, including fraud and money-laundering, and to analyze and manage other commercial risks;
- Enhance your customer experience;
- Perform all our legal and/or contractual obligations to you.

If you agree, we will share your data with our affiliates, related entities and business partners as stated hereunder so that they may offer you their products and services:

- The Insular Life Assurance Company, Ltd.;
- Lifestyle Partners. (Link to https://icare.com.ph/our-partners/lifestyle-partners/) You can inform us at any time if you no longer consent to cross-selling and cross-marketing;

**2. Other Uses by Nature of our Dealings**

Aside from the general uses stated above, we will use your personal information depending on your dealings with us, in any of the following:

When you inquire, solicit proposal and/or enter into a contract for HMO coverage with us:

- To conduct appropriate due diligence checks as required by IC, AMLC and other regulatory bodies. (Rule 18 – Customer Due Diligence, IRR of AMLA);
- To register your inquiry and address any follow-up calls;
- To prepare all necessary sales documentation and any other documentation as may be requested;
- To perform all financial processes related to contracting or renewal of HMO coverage;

- For corporate accounts: to publish your relevant information in our list of clients;
- To perform all our legal and/or contractual obligations to you;
- Other similar purposes.

When you apply for or become our director, officer or employee:

- To conduct appropriate background investigation. (Rule 16, IRR of AMLA);
- To conduct reference checks and pre-employment medical examination and interviews, and communicate with you the status of your candidacy;
- To be able to process your compensation, applicable allowances, bonuses, and expense reimbursements, and monitor your attendance and leaves;
- To enroll you in our benefit programs;
- To assist you in your professional development through performance management, career development, seminars, workshops and trainings;
- To make you part of our employee engagements, e.g. events, activities, and employee surveys and incentives;
- To comply with our obligations under the law as required by government instrumentalities including the BIR, DOLE and local government units;
- To facilitate, upon separation from the company, your exit interview, clearances, and other procedures necessary to process your final pay;
- To perform all our legal and/or contractual obligations to you;
- Other similar purposes.

When you are a prospective or current vendor, supplier, contractor or agent:

- To conduct appropriate due diligence checks as required by IC, AMLC and other regulatory bodies. (Rule 16, IRR of AMLA);
- To evaluate your proposal;

- To assess your viability as a vendor, supplier, contractor or agent, and process your accreditation;
- To communicate with you about matters relating to our required products and services;
- To comply with our obligations under the law as required by government instrumentalities including the BIR and local government units;
- To perform all our legal and/or contractual obligations to you;
- Other similar purposes.

When you seek accreditation or become our accredited health care provider:

- To conduct appropriate due diligence checks as required by IC, AMLC and other regulatory bodies. (Rule 16, IRR of AMLA);
- To communicate with you the status of your accreditation;
- To publish your relevant information in our roster of accredited health care providers;
- To be able to process relevant fees;
- To comply with our obligations under the law as required by government instrumentalities including the BIR and local government units;
- To perform all our legal and/or contractual obligations to you;
- Other similar purposes.

In any of the above instances, we commit to adhere with the principles of **transparency, legitimate purpose, proportionality and data quality.**

**How and where do we store your data?**

It is our policy that personal data shall only be stored in a properly managed environment with reasonable and appropriate organizational, physical, technical, administrative, procedural and security measures to protect it against security breach, as prescribed by law.

Physical copies of documents containing your personal information are stored in a sealed and secure manner in our Head Office at the following address:

**Insular Health Care, Inc. – Head Office**

2/F Insular Health Care Building, 167 Dela Rosa St. cor. Legazpi St., Legazpi Village, Makati City 1229, Metro Manila, Philippines Phone:(632) 8813-0131 Fax: (632) 813-7903

For inactive files which we must keep during the retention period (see: "How long will we keep your data?"), we utilize an Offsite Document Storage Facility by the following third-party provider which also implements reasonable and appropriate organizational, physical, technical, administrative, procedural and security measures to protect personal data against security breach, as prescribed by law:

**Crown Worldwide Movers, Inc.** Phase 7A Lot 5 Block I Laguna Technopark Binan Laguna Phone: (632) 822-1123

**How do we protect your data?** Our systems and storage medium and repositories that store personal data continuously undergo the appropriate information security, risk, legal compliance, and privacy impact assessments.

**To whom shall we disclose or divulge your data** As a rule, we shall not disclose nor divulge your data other than to persons whom you have specifically authorized or requested to receive them.

However, we may disclose or divulge your data **whether or not** you have given your specific consent, in any of the following instances:

- The disclosure or processing is necessary for compliance with a legal obligation to which we are subject (Sec. 12c, DPA);

- The disclosure or processing is necessary in order to respond to national emergency, or to comply with the requirements of public order and safety (Sec. 12e, DPA);
- The disclosure or processing is necessary for purposes of our legitimate interests or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms which require protection under the Philippine Constitution (Sec. 12f, DPA);
- The disclosure or processing of your personal data is provided for by existing laws and regulations: *Provided,* that such regulatory enactments guarantee the protection of the sensitive personal information and the privileged information: *Provided, further,* That your consent is not required by law or regulation permitting the disclosure or processing of the sensitive personal information or the privileged information (Sec. 13b, DPA);
- The disclosure or processing is necessary to protect your vitally important interests, including your life and health or that of another person, and you are not legally or physically able to express your consent prior to the disclosure or processing (Sec. 12d and Sec. 13c, DPA);
- The disclosure or processing is necessary for purposes of medical treatment, is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal information is ensured (Sec. 13e , DPA);
- The disclosure or processing concerns such personal information as 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 (Sec. 13f, DPA). (See: When are we obliged to disclose your data even without your consent?)

We also disclose or divulge your data to our vendors, suppliers and contractors that we engaged to help us carry out our legal and/or contractual obligations to you. In such case, we execute a **data sharing agreement** and make sure that our vendors, suppliers and contractors have proper safeguards in place to ensure the confidentiality of your personal data, prevent its use for unauthorized purposes, and generally, comply with the requirements of the DPA and other laws for processing of personal data. (Sec. 14, DPA)

**When are we obliged to disclose your data even without your consent?**

As an Insurance Commission Regulated Entity (ICRE), we are required to disclose or divulge your data to the AMLC **whether or not** you have given your specific consent, in any of the following instances:

- Cases falling under Republic Act No. 9160 or the Anti-Money Laundering Act of 2001, when there is probable cause that the payments involved are in anyway related to the following unlawful activities or a money laundering offense:
- Cases falling under Sections 4-16 of Republic Act No. 9165 or the Comprehensive Dangerous Drugs Act of 2002;
- Cases falling under Sec. 3 of Republic Act No. 3019 or the Anti-Graft and Corrupt Practices Act;
- Cases of plunder under Republic Act No. 7080;
- Cases of qualified theft under Art. 310 of the Revised Penal Code;
- Cases of swindling under Art. 315, and other forms of swindling under Art. 316 of the Revised Penal Code;
- Cases of smuggling under Republic Act No. 455 and Republic Act No. 1937 or the Tariff and Customs Code of the Philippines;
- Violations under Republic Act No. 8792 or the Electronic Commerce Act of 2000;
- "Destructive arson" and "murder" as defined under the Revised Penal Code;
- "Terrorism" and "conspiracy to commit terrorism" as defined and penalized under Republic Act No. 9372;
- "Financing of terrorism" under Sec. 4 and offenses punishable under Sec. 5-8 of Republic Act No. 10168 or the Terrorism Financing Prevention and Suppression Act of 2012;
- "Bribery" under Articles 210, 211 and 211-A of the Revised Penal Code;
- "Corruption of public officers" under Art. 212 of the Revised Penal Code;
- "Frauds and illegal exactions and transactions" under Articles 213-216 of the Revised Penal Code;
- "Malversation of public funds and property" under Art. 217 and Art. 222 of the Revised Penal Code;

- “Forgeries” and “counterfeiting” under Articles 163, 166, 167, 168, 169 and 176 of the Revised Penal Code;
- Violation of Presidential Decree No. 1612 or the Anti-Fencing Law;
- Violation of Republic Act No. 8293 or the Intellectual Property Code of the Philippines;
- Violation of Sec. 4 of Republic Act No. 9995 or the Anti-Photo and Video Voyeurism Act of 2009;
- Violation of Sec. 4 of Republic Act No. 9775 or the Anti-Child Pornography Act of 2009;
- Violation of Sections 5, 7-9, 10 (c), (d) and (e), 11-12, and 14 of Republic Act No. 7610 or the Special Protection of Children Against Abuse, Exploitation and Discrimination;
- Fraudulent practices and other violations under Republic Act No. 8799 or the Securities and Regulation Code of 2000
- Felonies or offenses of a nature similar to the aforementioned unlawful activities that are punishable under the penal laws of other countries.

Like any other person or corporation, we are also required to disclose or divulge your data to the government **whether or not** you have given your specific consent, in any of the following instances:

- When we are required, through a subpoena, to attend and testify at the hearing or the trial of an action, or at any investigation conducted by competent authority, or for the taking of deposition, or otherwise required to bring any books, documents or other things under our control (Rule 21, Sec. 1 of the Rules of Court) unless the personal data involved is considered privileged (Rule 130, Sec. 24 of the Rules of Court). In any of such cases, we shall, prior to or immediately after complying with the subpoena, inform you that we have been required to disclose your personal data so that you may avail of any available legal remedies to protect the same;
- For employees: when required by law to report transactions involving your personal data to the BIR. These include submission of BIR Form 1604F or the Annual Information Return of Income Taxes Withheld on Compensation which consist of

the summary of withholding tax on compensations (BIR Form 1601C) paid and filed to the BIR during the taxable year as well as the summary list (alphalist) of employees, existing and resigned, during the taxable year; and BIR Form 2316 or the Certificates of Compensation Payment/ Tax Withheld which details an employee's income earned, with the corresponding tax withheld and remitted to the BIR;

- For directors and officers: when required by law to submit a report to the SEC and IC. These include the submission of the General Information Sheet which contains personal information of directors and officers. (Sec. 25 of Republic Act No. 11232 or the Revised Corporation Code of the Philippines;
- For medical personnel and accredited health care providers: when required to furnish the Bureau of Working Conditions with copies of your contracts as well as records of all medical examinations, treatments and medical activities. (Art. 37, Labor Code; Rule I, Sec. 10, IRR of the Labor Code);
- For employees: when circumstances require the submission of an Establishment Report pursuant to Art. 297 (formerly numbered 282) of the Labor Code.

**How long will we keep your data?**

Unless sooner requested in writing (but subject to limitations), we will retain your personal data during the existence of our relationship (e.g. business, employment, agency) and until after the end of the following period:

| Data Involved | Period of Retention | Legal Basis |
|---|---|---|
| Records relating to an action upon a written contract, upon an obligation created by law and upon a judgment | 10 years | Art. 1144, Civil Code |
| Records relating to an action upon an oral | 6 years | Art. 1145, Civil Code |

| | | |
|---|---|---|
| contract and upon a quasi-contract | | |
| Records relating to an action upon an injury to the rights of the plaintiff and upon a quasi-delict | 4 years | Art. 1146, Civil Code |
| Receipts, Sales and Commercial Invoices | 3 years from the close of taxable year in which such invoice or receipt was issued | Sec. 5, National Internal Revenue Code |
| Records relating to gross income of employees | 5 years | Sec. 5, National Internal Revenue Code in relation to Sec. 281, National Internal Revenue Code |
| Records relating to violations of the National Internal Revenue Code | 5 years | Sec. 281, National Internal Revenue Code |
| Records of all transactions, including the full and true identity of customers and their customer identification documents | 10 years | Rule 18 – Customer Due Diligence, IRR of AMLA in relation to Art. 1144, Civil Code |
| Logbook of Sicknesses, Injuries and Death of Employees | 3 years | Art. 37, Labor Code; Rule I, Sec. 10, IRR of the Labor Code in relation to Art. 290, Labor Code |

| | | |
|---|---|---|
| Records relating to a claim for employees' compensation | 3 years | Rule VII, Sec. 6, IRR of the Labor Code; ECC Resolution No. 2799 |
| Workers Compensation | 1 year | Rule II, Sec. 3, IRR of the Labor Code |
| Individual time record of employees | 3 years | Art. 290, Labor Code |
| Records relating to a cause of action under the Labor Code | 3 years | Art. 290, Labor Code |

**How will we dispose your data?**

After the period mentioned above or as soon as you have requested us for the erasure, destruction and/or disposal of your personal data (but subject to limitations), the same shall be disposed in a secure manner that would prevent further processing, unauthorized access, or disclosure to any other party or the public.

For print out or other tangible formats, documents containing your personal data shall be shredded. For personal data in electronic form, pertinent documents shall be deleted, wiped, overwritten or otherwise made irretrievable

**What are your data protection rights?**

We would like to make sure that you are fully aware of all your data protection rights. As a data subject, you are entitled to the following:

- **Right to be informed**– You have the right to be informed whether personal information pertaining to you are being or have been processed. (See: "What data do we collect?" and "How do we collect your data?")
- **Right to access**– You may request for copies of data we hold about you by accomplishing our "Request for Production, Copying and/or Erasure of Data Form".
- **Right to object** – You may object to our processing of your personal data by withholding or withdrawing your consent or otherwise informing us about your objection. However, this may hinder us from fulfilling our legal and/or contractual obligations to you, or from properly responding to your concerns.

Please also note that as an ICRE and an AMLA covered institution, we are required to process certain personal information. As such, your exercise of this right may result in denial of HMO coverage.

Furthermore, as a health care provider, we may deny your right to object when processing is necessary to protect vitally important interests, including life and health, or whenever it is necessary in order for us to respond to a national emergency, to comply with the requirements of public order and safety, or otherwise perform legal obligations which necessarily include the processing of your personal data. (Sec. 12, DPA)

- **Right to restrict processing**– You may request us to restrict the processing of your personal data, under certain conditions.
- **Right to rectification and erasure** – You may request us to rectify and/or erase any or all data that we hold about you by accomplishing our "Request for Amendment, Correction and/or Erasure of Data Form".

However, in certain circumstances where the amendment, correction and/or erasure of data would adversely affect any person's freedom of speech or expression, contradict a legal obligation, act against public interest in the area of public health or in the area of scientific or historical research, or prohibit the establishment of a legal defense or exercise of other legal claims, we may not be able to amend, correct and/or erase the information subject of your request. In any of such cases, you will be informed promptly and given full reasons for the decision.

While in most cases we will be happy to amend, correct and/or erase the data subject of your request, we nevertheless reserve the right to refuse or charge a fee if the request is considered manifestly unfounded or excessive. In case of doubt regarding the propriety of your request, we may seek the opinion of the National Privacy Commission.

- **Right to data portability**– You may request us for the portability of your data by accomplishing our "Request for Data Portability and/or Erasure Form".
- **Right to assign**– Like other property rights, you may assign your rights as a data subject. Similarly, you may assert another person's rights as a data subject; *Provided,* that there is a valid assignment or designation. In any of such instances, we shall require for a copy of the data subject's written authorization as well as proof of the data subject and the assignee's identity.

For release of medical records to a person other than the data subject, please accomplish our "Request for Release of Medical Records Form".

- **Right to complain and claim damages**– If you feel that your personal data had been misused, maliciously disclosed, or improperly disposed, or that any of your data privacy rights had been violated, you may file a complaint by accomplishing our "Data Privacy Complaint Form".

You may also file a complaint and seek damages before the National Privacy Commission. (See: "How to contact the appropriate authorities?")

You may download other Data Privacy Forms here.

**Marketing**

We would like to send you information about our products and services that we think you might like, as well as those of our affiliates, related entities and business partners.

If you have agreed to receive marketing materials, you may always opt out later. You also have the right at any time to stop us from contacting you for marketing purposes or sharing your data to our affiliates, related entities and business partners.

If you no longer wish to be contacted for marketing purposes, click here.

**Changes to our privacy policy**

We keep our privacy policy under regular review and place any updates on this web page. This privacy policy was last updated on **28 November 2023**.

**Personal data breach management**

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 shall be subject to notification requirements under the following conditions:

- Compromised data involves personal data that may be used to enable identity fraud;
- There is reason to believe that the information may have been acquired by an unauthorized person; and
- The unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.

We shall notify the National Privacy Commission and affected data subjects in case of breach within 72 hours upon our knowledge of or reasonable belief that a personal data breach has occurred. If such event occurs, we shall notify you, through a secure means of

communication, of the nature of the breach, your personal information possibly compromised, measures taken to address the breach and reduce negative consequences, contact details of government authorities concerned and our Data Protection Office who can assist you in mitigating the possible ramifications that can compromise you and your right to privacy.

**How to contact the appropriate authorities**

The **National Privacy Commission** is the government office of the Republic of the Philippines in charge of the enforcement of all laws related to data privacy. It is ready at all times to assist the general public in matters pertaining to data privacy. For any inquiries or complaints, please contact the Public Information and Assistance Division of the National Privacy Commission at 5th Floor Delegation Building, PICC Complex, Roxas Boulevard, Pasay City with Trunk line No: 234-22-28 and email address: complaints@privacy.gov.ph

The official website of the National Privacy Commission is www.privacy.gov.ph

The **Insurance Commission**, with offices in Manila, Cebu and Davao, is the government office of the Republic of the Philippines in charge of the enforcement of all laws related to Health Maintenance Organization (HMO), and has supervision over HMOs like Insular Health Care. It is ready at all times to assist the general public in matters pertaining to HMO, pre-need and insurance. For any inquiries or complaints, please contact the Public Assistance and Mediation Division (PAMD) of the Insurance Commission at 1071 United Nations Avenue, Manila with telephone numbers +632-5238461 to 70 and email address: publicassistance@insurance.gov.ph

The official website of the Insurance Commission is www.insurance.gov.ph

**II. Processing of personal data on our website**

**Cookies**

Cookies are small files placed on your electronic device to collect standard Internet log information and visitor behavior information. When you visit our websites or use any of our digital apps, we may collect information from you automatically through cookies or similar technology.

**How do we use cookies?**

We use cookies in a range of ways to improve your experience on our websites, including:

- Keeping you signed in;
- Understanding how you use our websites;

- Showing you content as well as products and services that we may find relevant to you.

**What types of cookies do we use?**

There are several different types of cookies. Our websites use the following:

- Functionality – We use cookies so that we can recognize you on our websites and remember your previously selected preferences;
- Advertising – We use cookies to collect information about your visit to our websites, the content you viewed, the links you followed and information about your browser, device, and your IP address. (See: "Additional data collection activities")

**How to manage cookies**

You can change your cookie settings by opting out of all cookies. You may block cookies by changing the settings on your browser. However, if you choose not to permit cookies, our websites may not function properly or be accessible. Unless you have adjusted your browser settings so that it refuses cookies, we will drop cookies as soon as you visit our websites. This consent will expire periodically and in all cases within 365 days. If you wish to withdraw your consent at any time, you will need to delete all the cookies using your internet browser settings. Information about the procedure to follow in order to manage cookies can be found at:

- Chrome: https://support.google.com/chrome/answer/95647?hl=en
- Safari: https://support.apple.com/kb/PH19255?locale=en_US
- Safari Mobile: https://support.apple.com/en-us/HT201265
- Firefox: https://support.mozilla.org/en-US/kb/delete-cookies-remove-info-websites-stored
- Microsoft Edge: https://support.microsoft.com/en-us/help/17442/windows-internet-explorer-delete-manage-cookies

For more information on cookies, please visit www.allaboutcookies.org

To opt-out of participating in Google Analytics data, follow the instructions here: https://tools.google.com/dlpage/gaoptout

**Additional data collection activities (automated access)**

We receive and record information about the use of our websites either directly or through third-party tracking utility providers. These include collection of IP addresses, your

browsing behavior within and throughout our digital assets, and session lengths that are collected by our website analytic tools and cookies that we may place on your computer. You can disable the use of cookies on your browser at any time.

When you visit our website, we recognize only your domain name and not your email address. We will see your email address only if you provide it or send us an email message.

We do not ask you for, access or track any location-based information from your device. If we wish to do so in the future, we will specifically ask your permission.

**International Data Transfers**

1. **Third-Party Web Developer** – Our websites are managed and administered by a third-party web developer whose data base is in Singapore. By using our website, you consent (1) to the processing of your personal data and (2) that is shall be subject to cross-border data transfer. Upon your express written request, such cross-border transfer may be revoked at any time.
2. **Cloud Services** – Information that we collect may be stored and processed in and transferred between any of the countries where we make use of cloud services in order to enable us to use the information in accordance with this policy.
3. **Internet** – Personal information that you publish on our websites or submit for publication on our websites may be available, via the internet, around the world. We cannot prevent the use or misuse of such information by others.

**Payment processors**

We provide paid products and/or services on our websites, and use third-party services for payment processing (e.g. payment processors).

We will not store or collect your payment card details. That information is provided directly to our third-party payment processors whose use of your personal information is governed by their privacy policy.

**Privacy policies of other websites**

Our website and digital apps contain links and details of third-party websites. We have no control over, and are not responsible for, the privacy policies and practices of third parties. We therefore advise you to study their privacy policies. Once you leave our websites and digital apps, you should check the applicable privacy policy of third-party websites and digital apps to determine what information they will collect from you and how they will handle them.


**How to contact us**

Click here for the contact information of all our offices.

**How to contact our Data Privacy Officer**

If you have any questions, concerns, queries, comments, complaints about our privacy policy, the personal data we hold about you, or you would like to exercise any of your data protection rights, you may address them to iCare's Data Protection Officer at Insular Health Care – Data Protection Office, 2F Insular Health Care Bldg., 167 Dela Rosa St. cor. Legazpi Village, 1229 Makati City or via email at dataprivacy@insularhealthcare.com.ph