

Personal Data Processing Policy

PREMIUM CARE PLASTIC SURGERY S.A.S.

INTRODUCTION

The Political Constitution, Law 1581 of 2012 and Regulatory Decree 1377 of 2013 regulate the protection of personal data in Colombia. Personal data is any information linked to or associated with one or more specific or determinable natural persons, such as name, age, sex, marital status, domicile, among others, and in accordance with these rules, all persons have the right to know, update and rectify all types of information collected or that have been the subject of personal data processing in banks or databases and in general in archives of public and / or private entities.

Likewise, those responsible for the personal data processing are obliged to adopt an internal policy and procedures manual to guarantee the attention of queries and claims that the Data Holders have with respect to the treatment given to them.

PREMIUM CARE PLASTIC SURGERY S.A.S. (from now on PREMIUM CARE) has collected, stored and used information with personal data, and for its corporate purpose wishes to continue such treatment in the future. To this end, and in compliance with the Colombian legislation regarding the protection of personal data, it informs all interested parties the adoption of the following policies on the collection, processing and use of personal data, which will be mandatory for PREMIUM CARE, as Responsible for the treatment, its employees, as well as those third parties that by obligation and / or PREMIUM CARE disposition assume the quality of treatment managers or have access to them.

PREMIUM CARE must obtain the authorization so that its users, patients, clients and any other person who is immersed in relations with it, can freely collect, store, use, process, compile, update and dispose the data they have supplied and which have been incorporated in different databases, or electronic repositories. This information is and will be used in the development of the corporate purpose of PREMIUM CARE, as a legal person that provides health services, as well as for administrative, commercial, promotion and contact purposes with the holders thereof.

1. DEFINITIONS

2. PRINCIPLES OBSERVED BY PREMIUM CARE FOR THE PERSONAL DATA PROCESSING

3. DATA HOLDERS RIGHTS

4. PREMIUM CARE DUTIES WHEN ACTING AS RESPONSIBLE FOR DATA PROCESSING

5. PREMIUM CARE DUTIES WHEN ACTING AS A TREATMENT MANAGER

6. WHO CAN GET ACCESS TO THE HOLDER'S INFORMATION

7. PROCEDURE AND EXISTING CHANNELS TO RESPOND REQUESTS, CONSULTATIONS AND CLAIMS

7.1 Procedure to Respond Requests and Consultations related to the Personal Data Processing

7.2 Procedure to Respond Claims related to the Personal Data Processing

7.3 Responsible Area for the Attention of Requests, Inquiries and Claims

8. TREATMENT TO WHICH THE PERSONAL DATA AND THEIR PURPOSE WILL BE SUBMITTED

8.1 Personal data processing purpose for which PREMIUM CARE is responsible

8.2 Sensitive data PREMIUM CARE is responsible for

8.3 Treatment of children and adolescent's personal data

9. VALIDITY OF THE PERSONAL DATA'S HOLDERS PROCESSING POLICY

This Policy is published on the website for the Personal Data's holders treatment, such as patients, clients, suppliers, contractors, shareholders and employees of PREMIUM CARE; In accordance with the provisions of Law 1581 from 2012, and in the rules that modify, add or complement.

1. DEFINITIONS

For the purposes of this Policy, it is understood:

Authorization: Prior expressed and informed consent of the Holder to carry out the personal data processing. The authorization must be obtained through a physical or electronic document, text message, Internet, website, or also in a verbal or telephone or any other format that allows its subsequent consultation in order to verify unequivocally that without the consent, data would never have been captured and stored on electronic or physical media. Likewise, it may be obtained by means of clear and unequivocal conduct of the Holder that allows a reasonable conclusion that he gave his consent to the handling of his Personal Data.

Database: Organized set of personal data, either physically or electronically, that is subject to Treatment.

Personal data: Any information linked to or associated with one or more specific or determinable natural persons.

Public Data: Data that is not semi-private, private or sensitive, that can be treated by any person, without authorization. Data on the civil status of persons and those contained in public documents, on public records, on official gazettes and bulletins, and on enforced judicial decisions that are not subject to reservation are public, among others.

Semiprivate personal data: These are data that do not have an intimate, reserved, or public nature and whose knowledge or disclosure may interest not only the owner, but a group of people or society in general. For its treatment requires the express authorization of the holder of the information, for example, financial and credit data.

Sensitive Data: They are those that affect the holder's privacy or whose improper use can

generate their discrimination, such as those that reveal racial or ethnic origin, political orientation, religious or philosophical beliefs, membership in trade unions, social organizations, human rights or that promotes the interests of any political party or that guarantee the rights and guarantees of opposition political parties as well as data relating to health, sexual life and biometric data.

Treatment Manager: Natural or legal person, public or private, that by itself or in association with others, perform the personal data processing on behalf of the Responsible for Treatment.

Responsible for Treatment: Natural or legal person, public or private, that by itself or in association with others, decides on the data base and / or the data processing.

Habeas Data: Right of any person to know, update and rectify the information that has been collected about them in data banks and in archives of public and private entities.

Holder: Natural person whose personal data is subject to Treatment.

Treatment: Any operation or set of operations on personal data, such as the collection, storage, use, circulation or deletion.

Transference: The data transfer takes place when the person in charge and / or person in charge of the processing of personal data, located in Colombia, sends the information or the personal data to a receiver, who in turn is responsible for the treatment and is inside or outside the country.

Transmission: Processing of personal data that implies the communication thereof within or outside the territory of the Republic of Colombia when it is intended to carry out a treatment by the manager on behalf of the responsible.

2. PRINCIPLES OBSERVED BY PREMIUM CARE FOR THE PERSONAL DATA PROCESSING

Legality: The Treatment is a regulated activity that must be subject to the established in the Law.

Purpose: The Treatment must obey a legitimate purpose in accordance with the Constitution and Law, which must be informed to the Holder.

Reasonable limit: The storage and processing of personal data will be limited to what is essentially necessary to fulfill the previously specified purposes of the business relationship, as well as the fulfillment of the purposes authorized by the Holder.

Liberty: The Treatment can only be exercised with the prior, expressed and informed consent of the Holder. Personal data may not be obtained or disclosed without prior authorization, or in the absence of a legal or judicial mandate that relieves the consent.

Veracity or quality: The information subject to Treatment must be truthful, complete, accurate, updated, verifiable and understandable. Processing of partial, incomplete, fractional or error-inducing data is prohibited.

Transparency: The right of the Holder to obtain information from the Treatment Manager or Treatment Responsible, at any time and without restrictions, about the existence of their personal.

Access and restricted circulation: The Treatment may only be done by persons authorized by the Holder or by persons provided for in the Law. Personal data, except for public information, may not be available on the Internet or other means of mass communication, unless access is technically Controllable to provide restricted knowledge only to the Holders or third parties authorized pursuant to this law.

Security: The information must be handled with the human and administrative technical measures necessary to provide security for the records and prevent their adulteration, loss, consultation, use or unauthorized or fraudulent access.

Confidentiality: The personal data that do not have the nature of public are reserved, even after their relationship with any of the tasks included in the Treatment has ended, and only the supply or communication of personal data can be performed when this corresponds to the development of the authorized activities in the Present law and in the terms thereof.

Systematic incorporation: The principles of Personal Data Protection will be implemented in all business processes and procedures.

3. DATA HOLDERS RIGHTS

Personal data's holders have the right to:

- Know, update and rectify their personal data with the Treatment Managers or in charge of the Treatment. This right may be applied to all partial, inaccurate, incomplete, fractioned, misleading data or those whose Treatment is expressly prohibited or has not been authorized.
- Request proof of the authorization granted to the Person Responsible for Treatment, except when expressly excepted as a requirement for the Treatment or as established by applicable rules.
- Be informed by the Treatment Manager or Responsible, upon request, regarding the use that they have given to their personal data.
- Submit to the Superintendence of Industry and Commerce complaints for violations of the Data Protection Law or those that modify, add or complement it.

- Revoke the authorization and / or request the deletion of the data when: (i) In the Treatment, the principles, rights and constitutional and legal guarantees are not respected, provided that the Superintendence of Industry and Commerce has determined that in the Treatment, the Responsible have engaged in conduct contrary to ordination; And / or (ii) request it voluntarily, unless there is a legal or contractual obligation that imposes the obligation to remain in the database.
- Access free of charge your personal data that have been processed.

4. PREMIUM CARE DUTIES WHEN ACTING AS RESPONSIBLE FOR DATA PROCESSING

When PREMIUM CARE is responsible for the holder's data processing, it must fulfill the following duties:

- Guarantee the holder at all times, the full and effective exercise of the right of habeas data;
 - Request Authorization to the Holder informing:
 - The Treatment to which they will be submitted their personal data and the purpose of it.
 - The optional nature of the answer to the questions that are asked, when they are about sensitive data or about the children and adolescent's data.
 - The rights that assist as Holder.
 - The identification, physical or electronic address and telephone number of the Treatment Manager.
- Keep a copy of the Authorization granted by the Holder.
- Deliver a copy of the Authorization when the Holder or who is authorized, request it.
- Inform the Holder about the purpose of the collection and the rights that attend to him on the occasion of his Authorization.
- Keep the information under the necessary security conditions to prevent its adulteration, loss, consultation, use or unauthorized or fraudulent access.
- Ensure that the information provided to the Treatment Agent is truthful, complete, accurate, up-to-date, verifiable and comprehensible.
- Update the information, communicating in a timely manner to the Treatment Manager, all the updates from the Data that he has previously provided and take the necessary measures to ensure that the information provided to him is kept up-to-date.
- Correct information when it is incorrect and communicate the pertinent information to the Treatment Manager.
- Supply to the Treatment Manager, only Data who's Treatment is previously authorized.
- Require the Treatment Manager to respect the conditions of security and privacy of the Holder's information.
- To process the queries and claims made by the data owners within the terms established in this Policy.

- Inform the Data Treatment Responsible when certain information is being discussed by the Holder, once the complaint has been filed and the respective procedure has not been completed.
- Report at the request of the Holder the use given to his data.
- Inform the Superintendence of Industry and Commerce, or whoever is the data protection authority, when there are violations of the security codes and there are risks in the management of the Holder's information.
- Comply with the instructions and requirements of the Superintendence of Industry and Commerce.

5. PREMIUM CARE DUTIES WHEN ACTING AS A TREATMENT MANAGER

When PREMIUM CARE acts as a Treatment Manager, i.e., performs the treatment on behalf of a third party, it will fulfill the following duties:

- Guarantee the Holder, at all times, the full and effective exercise of the right of habeas data.
- Keep the information under the necessary security conditions to prevent its adulteration, loss, consultation, use or unauthorized or fraudulent access.
- Make opportunely the updating, rectification or deletion of the data in the terms established in this policy.
- Update the information reported by the Treatment Managers within five (5) working days of receipt.
- Handling the queries and claims made by the Holders.
- Register in the database the legend "complaint in process", when applicable;
- Insert in the database the legend "information under judicial discussion" once it is notified by the competent authority about judicial processes related to the quality of personal data.
- Refrain from circulating information that is being disputed by the Holder and whose blockade has been ordered by the Superintendence of Industry and Commerce.
- Allow access to information only to those who can access it.
- Inform the Superintendence of Industry and Commerce when there are violations of security codes and there are risks in the administration of the information of the Holders.
- Comply with the instructions and requirements issued by the Superintendence of Industry and Commerce.

6. WHO CAN GET ACCESS TO THE HOLDER'S INFORMATION

PREMIUM CARE will deliver the information on the Holder's Data to the following people:

- Holders, their assignees, their legal representatives or attorneys-in-fact;
- Public or administrative entities in the exercise of their legal functions or by court order;
- Third parties authorized by the Holder or by Law

7. PROCEDURE AND EXISTING CHANNELS TO RESPOND REQUESTS, CONSULTATIONS AND CLAIMS

The holders may exercise their rights to consult, know, update, rectify and delete their personal data by sending their request to the email info@premiumcareps.com, that request must contain at least:

- Application date.
- ID photocopy (citizenship card, institutional identification, etc.).
- Address for notification purposes.
- Person's signature requesting the information

7.1 Procedure to Respond Requests and Consultations related to the Personal Data Processing

Once the holder submits the request by the means indicated in this Policy, it will be dealt within ten (10) business days from the date of receipt. When it is not possible to attend the consultation within the aforementioned term, PREMIUM CARE will inform the interested party, stating the reasons and indicating the date of the consultation, no later than five (5) business days after the expiration of the first one.

7.2 Procedure to Respond Claims related to the Personal Data Processing

Through this procedure the Holder or who is authorized may make claims for:

- Update, modify, rectify or delete the data of the Holder.
- Revoke the Authorization of the Data Processing Holder, without prejudice to the standards that PREMIUM CARE must comply with regarding document retention. Consequently, PREMIUM CARE will delete the data or suspend its use when it is done, respecting the document conservation regulations that apply to it.
- Submit a complaint when it considers that there is an alleged breach of PREMIUM CARE's duties related to the Processing of Personal Data, in accordance with the provisions of these Policies or the Law on Protection of Personal Data and the norms that complement or modify it

The claim must be submitted in writing and must contain at least the following points:

- Full identification (name, notification address, identification document).
- Description of the facts that give rise to the query / complaint.
- Documents supporting the facts.
- Via for which you want to receive the answer to your inquiry / complaint.

In case of not having the previous information, it will be understood that the claim is not complete, in which case PREMIUM CARE will request the interested party to correct the faults or to send the information or documentation that is required.

PREMIUM CARE will respond to the claim within fifteen (15) business days from the day following the date of receipt. When it is not possible to deal with the claim within that term, the interested party will be informed the reasons for the delay and the date on which the claim will be dealt with, which shall not exceed eight (8) business days following the expiration of the first term.

8. TREATMENT TO WHICH THE PERSONAL DATA AND THEIR PURPOSE WILL BE SUBMITTED

8.1 Personal data processing purpose for which PREMIUM CARE is responsible

a) Patients and clients: The information will be used to develop PREMIUM CARE's corporate purpose, including providing medical care, sending diagnostic test results, providing PREMIUM CARE corporate, commercial and / or promotional information, always related to its corporate purpose on the health sector. As well as surveys to carry out satisfaction studies, news or corporate announcements that PREMIUM CARE may considers interesting.

In particular, the main purposes for the Personal Data Treatment that PREMIUM CARE will carry out in order to develop its corporate purpose are:

- Schedule appointments
- Processing of medical authorizations
- Delivery of medicines and medical equipment
- Replies to requests for improvements, petitions and complaints
- Generation of certifications in general
- Verification of affiliation status and services related to social security
- Educational Campaigns for the users
- Marketing activities and / or promotion PREMIUM CARE's services or its commercial partners for the provision of health services.
- Information on new products and services
- Information on campaigns and special programs
- Analysis of the general and individual population risk of data holders
- Analysis of health expenditure
- Definition of demand and analysis of services provided by PREMIUM CARE

- Audits
- Update of data and identification documents

The data related to the health of the patients will be strictly protected by PREMIUM CARE staff because of their sensitive nature, therefore, the following will be taken into account when processing data of this nature:

Medical - care personnel will access sensitive nature data because the holder expressed, prior and voluntary, this information, likewise, because of their professional practice will have knowledge of the patient 's medical history. Taking into account the protection required for this type of data, this information will be used for the exclusive purposes of providing health service and any other use must be expressly authorized. PREMIUM CARE employees are informed about the sensitivity of health data, the obligations and sanctions associated with their inappropriate use and the procedure to be followed in their treatment, the right of access by others other than the Holder, and how they are classified, communicated and delivered. They also know about the importance of not exposing medical results that may affect the person's privacy and not use the holder's personal data and affiliates outside the established medical or administrative purpose. Therefore, in PREMIUM CARE, the protection of information will not only be the responsibility of the medical - care staff, but also of all persons who have access to it in the exercise of their duties. PREMIUM CARE has a mechanism to prevent the leakage of sensitive information such as restriction on the use of removable media (CD, DVD), mail monitoring with attachments, real-time analysis of documents with malicious code (virus) through antivirus, PREMIUM CARE has a high-level CRM, called ZOHO, that meets all the global security requirements; Which offers a hierarchical system that allows the management of roles controlling the access to different sources of information to our employees. Likewise, we have a server with local connection, which avoids access to information outside our facilities.

In order to deliver medical results safely, it is essential that, when the holder cannot personally present himself or herself to obtain their results, send a written authorization stating the name of the authorized person, accompanied by a ID's photocopy of the holder as the authorized person, or present it personally for future occasions. The holder may also authorize their sending by email or certified mail.

b) Contractors and Suppliers: Their personal data will be used to carry out the development of the corresponding service provision contracts or other types of contracts, monitoring compliance and execution thereof. They will also be used to exchange information and publish PREMIUM CARE's portfolio. In addition, the data will be used to comply with the laws applicable to commercial relations between PREMIUM CARE and its contractors and suppliers.

The main purposes for which the personal data of the providers and providers will be treated are:

- Reports and requirements of control entities
- Generation of certifications in general
- Update of data and identification documents

c) Collaborators and workers: The personal data of ex-workers, current workers and candidates of PREMIUM CARE will be used to have a perception, both objective and subjective, about the personnel. Such information will be transferred and / or transmitted to other entities only when it is necessary to comply with the applicable legal provisions, in case it is required by public, administrative and / or supervisory bodies in labor matters in the exercise of their legal functions or by court order.

Collaborators and Workers' personal data processing will be done for verification of personal, commercial and labor information; Labor and Social Security aspects and those related to the contract that they celebrate or intend to celebrate with PREMIUM CARE, as well as will be used to control and prevent fraud.

8.2 Sensitive data PREMIUM CARE is responsible for

Law 1581 from 2012 prohibits the processing of sensitive data except in the following cases:

- When the Holder gives his / her consent explicitly and in advance. In this case, in addition to the general requirements of the authorization for the collection of any type of personal data, it should be established which of the data that will be object of treatment are sensitive and the purpose that will be given to them. The holder's health data will be considered part of their medical history and will have the reservation established in the law for this one.
- The Treatment is necessary to safeguard the vital interest of the Holder and is physically or legally incapacitated. In these events the representatives must grant their authorization.
- Treatment is carried out in the course of legitimate activities and with due guarantees by a foundation, NGO, association or any other non-profit making organization whose purpose is political, philosophical, religious or trade union, as long as they refer Exclusively to its members or to persons who maintain regular contacts by reason of their purpose.
- Treatment refers to data that are necessary for the recognition, exercise or defense of a right in a judicial process.
- The Treatment has a historical, statistical or scientific purpose, in the latter case the measures that lead to the suppression of the identity of the Holders must be adopted.

8.3 Treatment of children and adolescent's personal data

Law 1581 from 2012 prohibits the processing of children and adolescent's personal data, except for those that by their nature are public. However, the Constitutional Court stated that regardless of the nature of the data, it can be treated as long as:

- The aim pursued with such treatment is in the best interests of children and adolescents and
- Ensure, without exception, respect for your prevailing fundamental rights.

9. VALIDITY OF THE PERSONAL DATA'S HOLDERS PROCESSING POLICY

This Policy is available to Data Holders from June 2017.

Any substantial modification to it relating to the identification of the Responsible Party and to the purpose of the Treatment shall be communicated before implementing such change to the Holders through the website www.premiumcareplasticsurgery.com or any other efficient mechanism.