SINDUSFARMA Grupo de Trabalho Farmacovigilância Regional

SINDUSFARMA

LGPD: Impact for pharmacovigilance processes

Ana Luiza Torres, Arthur Soares Bueno, Bianca da Silva Bezerra Passos, Carolina Mazzine Said, Gislaine Dib, Itamar de Carvalho Junior, Raquel Simas Mazocolo, Rosana Mastellaro

I – INTRODUCTION

This document is intended for companies associated with SINDUSFARMA - Sindicato da Indústria de Produtos Farmacêuticos and aims to understand the impact of the General Data Protection Law – LGPD on the Pharmacovigilance Processes performed by them.

For guidance purposes only, the document was developed by a working group composed of representatives of the member companies, who analyzed, based on extensive experience with Pharmacovigilance, the main interactions of legal provisions and daily practice, without, however, exhausting the possibilities and topics.

Seeking a didactic model, the work group understood that the best way to provide guidance would be the dialectic, containing previously defined questions and answers, already carried out by some regulatory authorities with which the member companies maintain daily contact, such as, ANVISA - National Health Surveillance Agency.

Finally, being the guiding document, any and all companies will be able to adopt more flexible or restrictive internal criteria that best meet its interests, to comply with the obligations contained in LGPD.

II – COMPLIANCE TO LGPD

It is understood that the suitability of the Pharmacovigilance Processes to LGPD is based, in general, mainly on the following legal provisions:

> **ART. 7 THE PROCESSING OF PERSONAL DATA CAN ONLY BE PERFORMED IN THE FOLLOWING CASES:**
>
> **II – FOR THE COMPLIANCE OF LEGAL OR REGULATORY OBLIGATION BY THE CONTROLLER.**

- The laws in force at the time provide for the mandatory notification and monitoring of adverse events (AEs) occurred in patients in the period before and after marketing of drugs, vaccines and health products. Examples: RDC 406/2020; Normative Instruction 63/2020; RDC 09/2015; RDC 67/2009, among others.
- For topics involving Pharmacovigilance in clinical studies, it is recommended that the department responsible provide guidance considering the particularities of the area.

> **VII – FOR THE LIFE PROTECTION OR PHYSICAL SAFETY OF THE HOLDER OR THIRD PARTY.**

- The Pharmacovigilance Department is responsible for collecting and eventually sharing, especially with public authorities, information that can detect possible risks to the patient in the context of drug safety.

II.a. PERSONAL DATA ACCORDING TO LGPD

Personal data are considered, according to art. 5:

> **I – personal data:** information related to an identified or identifiable natural person;
>
> **II – sensitive personal data:** personal data about racial or ethnic origin, religious belief, political opinion, union membership or organization of religious, philosophical or political nature, data related to health or sexual life, genetic or biometric data, when linked to an individual;

II.b. DATA ANONYMIZATION

Anonymization is the removal of data that, individually or in combination, can lead to the identification of an individual. Data such as name, CPF (Taxpayer Identification Number), electronic device data and any other information that allows identification of the individual should be considered. According to art. 12 of LGPD, after anonymization, the data is no longer considered personal and, therefore, are not part of LGPD'S requirements.

> Art. 12. Anonymized data shall not be considered personal data for the purposes of this Law, except when the anonymization process to which it has been submitted is reversed, using exclusively proprietary means, or when it can be reversed with reasonable efforts.

Examples of the minimum personal data required for Pharmacovigilance purposes are: initials, gender, age and date of birth (considering the importance of these data to perform duplicate checking). For the purpose of contacting the reporter to follow-up the case, full name, e-mail and telephone number can also be collected. Please check section II.d. (Consent) for follow-up with a responsible health professional.

Therefore, for Pharmacovigilance purposes, it is considered:

Minimum personal data for the purpose of duplicate checking	Personal data required for case tracking purposes	Anonymized data, i.e., outside the LGPD scope
Initials	Name	-
Gender	Phone Number	Gender
Date of Birth	Email Address	Age

Exception: For underage patients, refer to specific topic below.

II.c. MINIMUM PERSONAL DATA REQUIRED TO COMPLY WITH PHARMACOVIGILANCE REGULATIONS

The company may, according to internal decision, collect the minimum necessary for compliance with Pharmacovigilance regulations without the need of consent. It is important to observe the principles of purpose and transparency (discussed in a specific topic below). Each company will be able to evaluate the minimum data that must be kept in the database to fulfill Pharmacovigilance activities (note database differences and specific scenarios, such as rare diseases, for example).

The minimum personal data for legal compliance with Pharmacovigilance activities can be kept in databases, always observing the principle of transparency and data access protection. Examples: initials, date of birth, age and gender, for duplicate checking purposes.

Note: To register the minimum data necessary to fulfill the Pharmacovigilance legal obligations, it is understood that, considering that the reporter, i.e, the person who notified the adverse event (AE) provides the information to the company, there will be no impediment to the registration of personal data. Therefore, there would be no need to request consent, as long as the principles of transparency are maintained, and the purpose related to Pharmacovigilance is maintained. For the follow-up of cases with the reporter, the same rationale is applicable, that is, there would be no obligation to collect consent. It will be up to each company to adopt a more conservative approach.

Is there any difference in the understanding of what can be in the source document and what can be in the structural fields of the database, considering the differences related to data sharing (ex: source document is not available globally)? Can personal data be kept anonymous only in structural fields or must it also be obliterated in the source document?

Answer: There is no difference. If the personal data can be registered in the database (i.e., if it is the minimum necessary for compliance with regulations and considering that the pharmacovigilance activity is a legal requirement and that aims to protect life), it can be in the source document and/or in the structural fields of the system. The company must ensure suitable protection of access to this data as well as transparency on how the data will be processed.

II.d. CONSENT

It is important to note the difference between what should be informed and what must be consented to. The reporter must be advised that the minimum personal data for fulfilling Pharmacovigilance activities will be registered, since this is a regulatory requirement. Unless it is necessary data for compliance with local regulations (for example, duplicate checking and follow up), consent must be requested regarding the registration of other personal data in the database, including information for contacting the responsible health professional, when he/she is not the primary reporter of the information or the use of the data for any other purpose.

Data from underaged should be treated as an exception (refer to specific topic below). Without the consent of the legal guardian, the company must not register information that enables identification of the patient, but anonymized data can be registered. **Refer to table above ("Data Anonymization" item) for examples of using minimum data to comply with pharmacovigilance and anonymization regulations.**

The company should inform the client in case of any change in relation to what had been previously informed about processing the data.

In case the reporter's contact to the company is made by e-mail or digital channels, the company may contact the client to follow up the case and register personal information, besides indicating where information can be found on how the data will be treated for the company.

However, if during the contact the patient informs that he/she does not authorize his/her personal data to be recorded, the notifier must be informed that the minimum necessary (examples: data for duplicate checking) to comply with Pharmacovigilance regulations will be maintained. In this case, it is recommended that the contact information be obliterated, examples: e-mail, telephone, full name. For the follow-up of cases with the reporter, the same rule applies. In cases where there is a need to contact the responsible health professional, authorization must be obtained.

Can we register personal data, even if it is as the minimum for duplicate checking purposes, without consent (just informing the client that this will be done), considering that it is indicated in Normative Instruction 63/2020 that the registration holders must have a process for check for duplicate notifications?

Answer: According to the legal basis "II – For the controller's compliance with legal or regulatory obligation" (art. 7) and Normative Instruction 63/2020 (or other current legislation that contains this type of requirement), which mentions that market authorization holders must have processes to verify duplication of notifications, it is possible to collect personal data from patients without the need of express consent, evidently considering all other principles of LGPD (purpose, suitability, necessity, quality, transparency, security, prevention and non-discrimination), including Art.10 § 1 When the processing is based on controller's legitimate interest, only the personal data strictly necessary for the intended purpose can be processed.

Additionally, it is important to reinforce the information contained in art 11.

Art. 11. The processing of sensitive personal data can only occur in the following cases:

II - without consent from the holder being given, in cases in which it is indispensable to:

a) compliance with a legal or

regulatory obligation by the controller;

If the notifier (not being the patient) provides the patient's data and authorizes them to be registered by the company, we can keep the patient's data in the database or the consent must always be provided directly by the person who will have their data registered (holder data)?

Answer: The same rationale indicated in the answer above applies when a third party contacts the company and provides personal data about another person (for example: reporter contacts the company reporting an adverse event that occurred with his/her brother).

Can the company call the patient/doctor, if the notifier (this being a third party) has authorized it?

Answer: It is understood that the authorization given by the notifier for contact with the health professional or person responsible for monitoring the case for a pharmacovigilance proposal would be enough by way of consent. The purpose of the contact should be clarified to the health professional or legal guardian.

II.e. PROCESSING OF PERSONAL DATA OF CHILDREN AND ADOLESCENTS

How should data received by the company directly by children or adolescents be processed when it is not possible to obtain parental or legal guardian consent?

Answer: Data from children or adolescents, even if they are the minimum necessary to comply with local regulations, cannot be recorded without parental or legal guardian's consent, being an exception to the rationale described above. If it is impossible to collect consent if the contact is made by the minor, the registration must be done anonymously, since anonymized data are not considered personal data. In this case, the follow-up would also not be applicable.

"Art. 12. Anonymized data shall not be considered personal data for the purposes of this Law except when the anonymization process to which it has been submitted is reversed, using exclusively proprietary means, or when it can be reversed with reasonable efforts.

"Art. 14. The processing of personal data of children and adolescents must be carried out in their best interest, under the terms of this article and the relevant legislation.

§ 1 The treatment of children's personal data must be carried out with the specific and highlighted consent given by at least one of the parents or the legal guardian.

§ 3 Personal data of children without the consent referred to in § 1 of this article may be collected when the collection is necessary to contact the parents or legal guardian, used once and without storage, or for their protection, and in no case if they may be passed on to third parties without the consent referred to in § 1 of this article.

§ 5 The controller shall make all reasonable efforts to verify that the consent referred to in § 1 of this article has been given by the responsible party of the child, considering the available technologies.

II.f. TRANSPARENCY

The holder of the personal data must have access to all applicable information related to data privacy and how her/his personal information will be handled. Each company must evaluate the strategies used to declare the transparency of data processing through the different channels (including sales force, e-mail, websites etc). Examples of strategies: verbal communication, IVR (Interactive Voice Response), website, information card, terms of use, standard response, etc. It is possible that the main parts of the information are in the IVR and the rest on the company's website (in this case, the IVR should inform that the customer can consult more details on the website x).

It is important to inform who the personal data will be shared with (e.g. different countries, regulatory authorities, business partners, etc.). This must be done at all information entry ways.

If the holder of the personal data requests removal of his/her data from the company's database, all data that can identify the customer must be removed, however, personal information may be kept in a minimally necessary manner to fulfill Pharmacovigilance activities.

Companies should have processes that allow identifying to which other internal sectors the information has been transmitted, so that all applicable records are deleted. That is, if the information is registered in the SAC - Customer Service - system and also in the Pharmacovigilance database, if the customer asks the SAC to remove the data, the Pharmacovigilance should be informed so that it also removes the applicable information records, maintaining only the minimum necessary to comply with local regulations.

II.g. DATA TRANSFER

If the data is going to be submitted to another country, to business partners or other pharmaceutical industries as a courtesy report in an anonymous way, do we still need to inform about the transfer? Or should this be done only if personal data is transmitted?

> **Answer:** Even if the transfer is made anonymously, it is recommended the principle of transparency to be followed, that is, the company could inform about the transfer of data. As long as they are anonymized, there is no need for consent, observing the principles described at the beginning of the document.

If the data will be transmitted to another country in a way that makes it possible to identify the data holder, what are the necessary requirements?

> **Answer:** If it is possible to identify the holder, it is necessary to comply with the rules provided in art. 33 of LGPD.
>
> Art. 33. The international transfer of personal data is only allowed in the following cases:
>
> I - for countries or international organizations that provide a degree of protection of personal data suitable to what is requested in this Law;
>
> II - when the controller offers and proves guarantees of compliance with the principles, the rights of the holder and the data protection system provided for in this Law in the form of:
>
> a) specific contractual clauses for a given transfer;
>
> b) standard contractual clauses;
>
> c) global corporate standards;
>
> d) stamps, certificates and codes of conduct regularly issued.

If the company has not received consent for registration of personal data and, therefore, has registered only the minimum data necessary to

comply with legal obligations, can this company share personal data with the regulatory authority? Can the company share this data in the notification of the individual case or only at the request of the regulatory authority??

Answer: The company cannot share personal data with the regulatory authority, unless there is a formal request from the regulatory authority. Notifications in general should be made anonymously.

II.h. AUDIT / INSPECTION

If the patient's personal data is recorded and an auditor or inspector requests access to the case information, what precautions should the company take?

Answer: In the event of an audit, the auditor must be prevented from having access to personal data. If it is not possible due to the purpose of the audit, the auditor may have access, as long as he/she signs a confidentiality term, as, for example, in the case of an external audit.

In case of inspections, the inspector may have access to the data, considering the applicable regulatory nature

II.i. SAFETY COMMUNICATIONS TO HEALTHCARE PROFESSIONALS

Based on the excerpt "VII - for the protection of the life or physical safety of the holder or third party. Assumption that the consent of the holder of the data is dispensed in cases of need to protect the greater good of the natural person, life and its safety, both inserted in the concept of human dignity as the foundation of the Republic", can we send safety alerts to physicians without their consent? What can we consider "protection of life"? To be sent without consent, does the material have to contain **only** information related to patient safety?

Answer: The Pharmacovigilance Department is responsible for collecting information that can detect potential risks to the patient in the scope of drug safety. Such risks, if identified, need to be disclosed to the entire medical public to be effectively communicated to patients. It is understood that this item complies with art. 7, as it aims to protect the life of the holder or third party, and therefore would dispense the consent of health professionals as to receive these security alerts from the Marketing Authorization Holders. It is recommended that companies evaluate how health professionals' data were obtained for the purpose of weighting risks involving LGPD requirements versus the need of disclosuring safety information.

"Art. 7 The processing of personal data can only be carried out in the following cases:

VII - for the protection of the life or physical safety of the holder or third party;"

It is important to note that the material must contain exclusively information related to patient safety, without any promotional content.

II.j. REMOVAL OF DATA FROM THE PHARMACOVIGILANCE DATABASE

If the customer requests the removal of data from the company's database, is it necessary to explain to the customer that the data cannot be deleted, but that only the minimum necessary data will be kept in the database? Does data removal need to be evidenced in any way for the patient?

Answer: The removal of data is not necessary in its entirety considering its strict use for the purpose of Pharmacovigilance, respecting the principles of purpose and transparency and provided that the minimum necessary to comply with the regulatory requirements pertinent to Pharmacovigilance is maintained. The client needs to have transparency on how his/her data will be treated and stored, and it is always necessary to inform him/her that the pharmaceutical industries have a legal requirement to follow the safety information of their products in the long term, therefore the personal data minimally necessary to fulfill relevant clinical information and regulations should be kept in the database.

"Art. 6: The activities of processing of personal data shall comply with the good faith and the following principles:

I - Purpose: to carry out processing for legitimate, specific, explicit and informed purposes to the holder, without the possibility of further processing in a way incompatible with those purposes;

VI - transparency: guarantee, to the holders, of clear, accurate and easily accessible information on the processing and the respective processing agents, subject to business and industrial secrets;

"Art. 7 The processing of personal data can only be carried out in the following cases:

II - for the compliance of legal or regulatory obligation by the controller;

After the 20 years provided for in the regulations for filing cases, do we need to delete personal data (considering that we will no longer have the legal basis)? Is there any difference if we still have the product on the market?

Answer: Considering that the security data is in a database with restricted access and specific purposes which govern the security monitoring and provision of safe products to its users, it is understood that there is no need to go back to the reports and anonymize or exclude all files after 20 years. The records in the Pharmacovigilance database are the basis for the information in several regulatory documents, so it would be difficult to guarantee the traceability of the data without the evidence from the files.

"Art. 16. Personal data will be deleted after the end of its processing, within the scope and technical limits of the activities, authorized the conservation for the following purposes:

I - the compliance with legal or regulatory obligations by the controller;

II.k. STANDARD VALIDITY

Will only data received by the company be considered after the law is in force? Can the customer request the removal of data recorded before the law came into effect?

Answer: Yes, the adjustments with respect to the data will be applied to the records received after the law is in force. However, if a new contact is received from a reporter who already has previously registered data and in this contact is requested to remove his/her data from the company's database, it must be informed that the minimum personal data must be kept complying with Pharmacovigilance, as explained in item II.j.

III. CONCLUSION

Since Pharmacovigilance is a regulatory obligation of the pharmaceutical industries and having this focus strictly related to patient safety, the legal bases cited in this guide are the most suitable for the treatment of personal data in this context, emphasizing the importance of guaranteeing data subjects the principles of LGPD, highlighting transparency and purpose..

It is recommended that only the minimum data required to fulfill Pharmacovigilance activities to be collected and that companies implement processes and systems that ensure the processing of personal data. Consent only becomes mandatory if the company chooses to collect personal data in addition to those considered to be minimal to comply with regulatory requirements, except for the collection of personal data from minors, in which the consent of those responsible is essential. It is worth emphasizing that the handling of anonymized data is outside the scope of this law.

This document was developed with guideline purposes regarding the analysis of the impacts of the General Data Protection Law for Pharmacovigilance activities. Companies have the autonomy to conduct additional analyzes in relation to the requirements of the law, and may adopt internal criteria that are more flexible or restrictive than those indicated in this guide, as long as they guarantee their proper compliance.

IV. COMPOSITION OF THE WORKING GROUP

Ana Luiza Torres – GSK

Arthur Soares Bueno – Sanofi Medley

Bianca da Silva Bezerra Passos – Sanofi Medley

Carolina Mazzine Said – Sanofi Medley

Gislaine Dib – Libbs

Itamar de Carvalho Junior – Sindusfarma

Raquel Simas Mazocolo – Sindusfarma

Rosana Mastellaro – Sindusfarma

EXPEDIENT

Publication of Sindusfarma - Pharmaceutical Industry Union / Content prepared the LGPD Impact Discussion Subgroup on Pharmacovigilance / Working Group on Pharmacovigilance, Regulatory Affairs Directorate / Responsible: Rosana Mastellaro, Director of Regulatory Affairs / sindusfarma.org.br.