Chile's new data protection law and its effects on health data privacy

Monday 2 June 2025

Ignacio Gillmore
Carey, Santiago
igillmore@carey.cl

Cristina Busquets
Carey, Barcelona
cbusquets@carey.cl

Camila Suárez
Carey, Santiago
csuarez@carey.cl

Introduction

In Chile, the recent enactment and publication of Law No. 21,719, which 'regulates the protection and processing of personal data and creates the agency for the protection of personal data', represents the most significant milestone in regard to data protection regulation in decades, as it significantly amends Law No. 19,628 (the 'Old Data Privacy Law' or oDPL).

Indeed, despite five amendments since its enactment in 1999, the oDPL largely retained its original structure, with minor adjustments, primarily concerning data associated with economic, financial or commercial obligations and its disclosure.

Now, Law No. 19,628 as amended by Law No. 21,719 (the 'New Data Privacy Law' or nDPL) provides a set of rules that innovates the processing bases, data protection principles and enforcement, including the creation of a Data Protection Agency with vast authority to investigate potential infringements, impose fines or corrective actions, etc, which is set to take effect on 1 December 2026.

In this context, the nDPL introduces changes to the regulation of health data, which we will briefly outline in this article to help inform stakeholders and encourage further discussions on the subject.[1]

Health data under the oDPL

Under the oDPL, there were only two legal bases for the processing of sensitive data, understood as 'personal data relating to a person's physical or moral characteristics, as well as facts or circumstances of their private life or intimacy, such as personal habits, racial origin, political ideologies and opinions, religious beliefs or convictions, physical or mental health status, and sexual life', namely when informed written consent has been secured from the data subject and in order to comply with the law (which included cases where the processing was necessary for determining or granting health benefits to the data subject).

Additionally, it recognised the patient's right to access their data; request its rectification if it was proven to be incorrect, inaccurate, misleading or incomplete; and request its cancellation (deletion) or blocking in the absence of legal grounds for its storage if the data was no longer necessary or if provided voluntarily and the subject no longer wishes for their data to be retained.

In such context, the oDPL established a terse legal framework for the processing of health data, relying on other sector-specific laws and regulations, such as Law No. 20,584 on patients' rights and duties, S.D. 41/2012 on medical records and Law No. 20,120 on biomedical research and its regulations. However, the scarcity of legal provisions, coupled with the absence of a dedicated authority and proper enforcement mechanisms, meant that data protection largely depended on other applicable laws and regulations. For instance, in the case of clinical trials, data protection was indirectly enforced through the Ethics Committee (EC) review process mandated by Law No. 20,120 in reference to the oDPL.

Health data under the nDPL

Under the nDPL, the legal landscape in which health data controllers act has been expanded, as it provides new processing bases, distinguishing between types of data, while, at the same time, the respective rights and obligations have been further developed, providing more clarity in regard to health data processing operations.

Processing bases and personal data categories

Paragraph 2 of Title II of the nDPL is dedicated to the processing of sensitive data, which is now defined as 'personal data relating to a person's physical or moral characteristics, or to facts or circumstances of their private life or intimacy, that reveal their ethnic or racial origin, political, trade union, or professional association affiliation, socioeconomic status, ideological or philosophical convictions, religious beliefs, health-related data, human biological profile, biometric data, and information concerning their sexual life, sexual orientation, or gender identity', while Paragraph 3 is dedicated to the 'special categories of personal data', as detailed below.

Paragraph 2 related to the processing of sensitive data:

- Article 16 – sensitive data in general;
- Article 16 bis – health-related data and biological profile, such as genetic, proteomic or metabolic data; also including an express mention to biological samples; and
- Article 16 ter – biometric data.

Paragraph 3 related to the processing of special categories of personal data:

- Article 16 quáter – data belonging to minors;
- Article 16 quinquies – data with historical, statistical, scientific and study or research-related purposes; and
- Article 16 sexies – geolocation data.

Each article indicates the applicable processing basis.

Health-related data

Now, focusing on health-related and biological profile data, eg, genetic, proteomic or metabolic data, the main processing basis is still consent, which may now be provided in writing, verbally or through an equivalent technological means. However, it is only required for a purpose that is recognised by a sanitary law (eg, biomedical research is recognised by Law No. 20,120, patient support programmes may be understood to be recognised by Article 100 of the Sanitary Code, etc).

However, there are six additional legal bases that can be used in regard to data processing in the context of healthcare, among which we highlight the following:

1. When the processing is indispensable to safeguard the life, physical or mental integrity of the subject or another person, or when the subject is physically or legally prevented from providing consent, in which case the subject shall be informed of the processing once the impediment disappears (Article 16 bis a).

Although the wording of this provision may not be completely clear, we can conclude that for the basis to be utilised it is necessary that there is a threat to a person's physical or mental health, who is prevented from providing consent at that moment.[2] Otherwise, this would pose a risk to the subject's rights as their health data could be otherwise processed by the controller, provided the subject is informed after the impediment disappears (which may never happen in some cases).

2. When the data is used for historical, statistical or scientific purposes, for studies or research with public interest purposes, for the benefit of human health or for the development of medical products that could not be developed otherwise (Article 16 bis c), which allows the publication of the results of such studies after anonymisation has taken place.

This basis may be useful for clinical trials as, although informed consent forms (ICFs) are still mandatory as per law No. 20,120, and enforced by ECs, in connection with the information that potential trial subjects must receive in order to validly consent to their enrolment, it could eventually be used to support data processing even when consent is poorly set forth in the ICF and, most interestingly, for secondary research purposes. This means that sponsors may not have to repeat the ICF process and may reduce the risks associated with such data processing activities, provided all the principles and obligations included in the nDPL are complied with (eg, conducting privacy impact assessments when applicable, adopting safety measures to protect the data, etc).

This basis is also developed by Article 16 quinquies, which recognises 'data with historical, statistical, scientific and study or research-related purposes' as a special data category. Here, the law presumes the existence of a legitimate interest in such data processing, provided these are the exclusive purposes of the processing, namely being of public interest. However, controllers must adopt sufficient quality and safety measures to guarantee respect for the processing purpose and, if sensitive data is involved, the controller must also assess the potential risks and measures for their mitigation. If the latter is complied with, the data may be stored and used for an undetermined period, and the results may be published after anonymization has taken place.

3. When the processing is necessary for purposes of preventive or occupational medicine, an assessment of a worker's fitness for employment, medical diagnosis, the provision of healthcare or social care services or the management of healthcare and social care systems and services (Article 16 e).
4. When the law states and indicates the purpose that the processing shall have (Article 16 f). For example, for the purpose of establishing medical records, as set forth by Law No. 20,584 and S.D. 41/2012.

Finally, the article sets forth a prohibition on processing health-related data and related biological samples (if they belong to an identified or potentially identifiable individual) when the data has been obtained in a context involving labour, educational, sports, social, insurance, security or identification, except when legal authorisation applies. In such regard, Article 16 e should be understood as an exception to this rule.

Other changes and effects on the healthcare industry

The new legal provisions are accompanied by the creation of several new obligations.

For example, the nDPL mandates that controllers conduct privacy impact assessments (PIAs) under certain circumstances, such as when processing sensitive data in cases where an exemption to consent applies, while the general rule refers to cases where the processing is likely to present a high risk to the rights of the subjects, due to its nature, scope, context, the technology used or purposes. However, given the scope of this rule, the Data Protection Agency will provide a referential list of circumstances, as well as guidelines and criteria to be followed. It will also be possible to consult with the Data Protection Agency about a specific case.

Other new obligations include adopting technical and organisational measures to comply with the nDPL and to guarantee that the purpose limitation and proportionality principles are respected; the adoption of safety measures to guarantee confidentiality, integrity, availability and resilience of the systems, according to the specific case, risk and potential impact; as well as reporting to the Data Protection Agency about any security breaches leading to the destruction, leak, loss or alteration of data that may pose a reasonable risk to data subjects' rights. If minors' or sensitive data is involved, it will also be mandatory to report the breach to the data subjects (either personally or through mass media). In any case, the respective compliance standards will be detailed by the Data Protection Agency.

In regard to data subjects' rights, please note that these are further developed by the nDPL, introducing the right to object (regarding automated decisions) and the right to data portability, in addition to those already recognised by the oDPL. However, the new law also establishes exceptions. For instance, cancellation requests are not applicable when the data processing is necessary for public interest activities or scientific research, studies or other purposes of public interest, and the same limitation applies to objections to processing.

On another note, the nDPL sets forth requirements for international data transfers and creates the abovementioned Data Protection Agency, granting it oversight of the relevant sanctioning regime. Indeed, fines are a key element of the nDPL as the oDPL only applied fines after a judicial proceeding had been completed and up to ten monthly tax units (UTM) (approx. $720 in April 2025), as a general rule. Under the nDPL, fines will be categorised as minor, serious or very serious infractions, risking fines of up to 20,000 UTM (approx. $1,441,600), among others (in the case of recidivism).

Final considerations

The nDPL represents a significant step towards affording the same level of protection as international standards, similar to Europe's General Data Protection Regulation. In regard to health data, stakeholders will have to deal with moving from being subject to very limited regulation, to having to address different potential processing bases and provisions that seem to recognise the relevance and value of, for example, clinical research and medical product development, while balancing such relevance with the rights and interests of data subjects.

Nevertheless, the new obligations set forth by the nDPL and the strict sanctions regime may pose challenges for local stakeholders, who will need to adapt their operations to this new legal landscape before the two-year commencement deferral ends, on 1 December 2026.

In any case, it will be key for stakeholders to closely monitor the actions and determinations of the new Data Protection Agency, as it has the authority to issue general guidelines and provide administrative interpretations of the law. In such regard, the Data Protection Agency may serve as a valuable ally in the ongoing management of health data processing in Chile.

Notes

[1] Please note that due to space constraints this article provides only a high-level overview of the key provisions within the nDPL and does not aim to comprehensively cover all of its innovations in comparison to the oDPL or all of the potential implications for health data processors.
[2] This may also be understood based on the comments registered in the nDPL's legislative history, page 641: '[…] Finally, he was willing to maintain the proposed wording, but only on the understanding that the scope of application of the provision is limited to cases of urgency. In the absence of such urgency, the data could not be processed without obtaining the necessary consent. The Honorable Senator Mr. Huenchumilla agreed with this analysis, as the very nature of the provision implies considering urgency.'