LATIN LAWYER INSIGHT

The Guide to Corporate Compliance

Editors
Andrew M Levine
Reynaldo Manzanarez Radilla
Valeria Plastino
Fabio Selhorst

Published in association with

LACCA
Latin American Corporate Counsel Association

© Law Business Research 2020

The Guide to Corporate Compliance

Editors
Andrew M Levine
Reynaldo Manzanarez Radilla
Valeria Plastino
Fabio Selhorst

Reproduced with permission from Law Business Research Ltd
This article was first published in June 2020
For further information please contact Natalie.Clarke@lbresearch.com

LATIN LAWYER

Published in association with
LACCA

© Law Business Research 2020

Publisher
Clare Bolton

Deputy Publisher
Rosie Creswell

Senior Account Manager
Monica Fuertes

Senior Content Coordinator
Hannah Higgins

Head of Production
Adam Myers

Production Editor
Caroline Fewkes

Subeditor
Martin Roach

Chief Executive Officer
Nick Brailey

Published in the United Kingdom
by Law Business Research Ltd, London
Meridian House, 34-35 Farringdon Street, London, EC4A 4HL, UK
© 2020 Law Business Research Ltd
www.latinlawyer.com

No photocopying: copyright licences do not apply.

The information provided in this publication is general and may not apply in a specific situation, nor does it necessarily represent the views of authors' firms or their clients. Legal advice should always be sought before taking any legal action based on the information provided. The publishers accept no responsibility for any acts or omissions contained herein. Although the information provided is accurate as of March 2020, be advised that this is a developing area.

Enquiries concerning reproduction should be sent to Law Business Research, at the address above. Enquiries concerning editorial content should be directed to the Publisher – clare.bolton@lbresearch.com

ISBN 978-1-83862-428-6

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

© Law Business Research 2020

Acknowledgements

The publisher acknowledges and thanks the following for their learned assistance throughout the preparation of this book:

Alvarez & Marsal, LLP

Andrew Jánszky

Anheuser-Busch InBev

Barbosa Müssnich Aragão

Beccar Varela

Buckley LLP

Camargo Corrêa Infra

Carey y Cía

Debevoise & Plimpton LLP

FeldensMadruga

Hogan Lovells

Kestener, Granja & Vieira Advogados

Maeda, Ayres & Sarubbi Advogados

Philippi Prietocarrizosa Ferrero DU & Uría

QIL+4 Abogados

Quinn Emanuel LLP

Reynaldo Manzanarez Radilla

© Law Business Research 2020

Skadden, Arps, Slate, Meagher & Flom LLP

Sullivan & Cromwell LLP

TozziniFreire Advogados

Villarreal-VGF

Von Wobeser y Sierra, SC

Whirlpool Corporation

© Law Business Research 2020

Publisher's Note

Latin Lawyer and LACCA are delighted to publish *The Guide to Corporate Compliance*.

Edited by Andrew M Levine, a litigation partner at Debevoise & Plimpton LLP, Reynaldo Manzanarez Radilla, a corporate attorney and compliance professional, Valeria Plastino, vice president, general counsel and regional ethics and compliance officer at CenturyLink, and Fabio Selhorst, general counsel, chief integrity officer and chief communications officer at Camargo Corrêa Infra, this new guide brings together the knowledge and experience of leading practitioners from a variety of disciplines and provides guidance that will benefit all practitioners.

We are delighted to have worked with so many leading individuals to produce *The Guide to Corporate Compliance*. If you find it useful, you may also like the other books in the Latin Lawyer series, including *The Guide to Infrastructure and Energy Investment* and *The Guide to Corporate Crisis Management*, as well as our jurisdictional references and our new tool providing overviews of regulators in Latin America.

My thanks to the editors for their vision and energy in pursuing this project and to my colleagues in production for achieving such a polished work.

© Law Business Research 2020

Contents

© Law Business Research 2020

© Law Business Research 2020

Part 5

Staying Compliant in Higher-Risk Industries

© Law Business Research 2020

20

Data Privacy and Protection Relating to Healthcare in Europe, the United States and Brazil

Fabio Alonso Vieira and Carolina Barbosa Cunha Costa[1]

Introduction

We are currently experiencing the third major global economic wave, described by Alvin Tofler as the 'Information Age',[2] in which information, knowledge and high-end technology are essential for the development and success of companies. We live in a completely digital world that allows instant and fluid communication. Information is an extremely valuable asset in this highly globalised market.

Owing to the fluidity with which information is shared today, individuals have begun to lose control over their privacy and personal details and, to some extent, can become victims of social networks, public databases, information migration and Big Data, among other things. In this context, there have been several discussions about how to implement an effective system for protecting individuals' data.

In particular, the healthcare sector has been using patients' medical information, such as that processed during clinical trials or patient programmes around the world, to develop through artificial intelligence new products and services. Beyond the medical context, healthcare companies (including those in the pharmaceutical sector) use all sorts of modern technologies to track and measure people's health, and to help them get into shape, keep fit, lose weight and reduce stress.

In our rapidly evolving digital world, technologies are advancing by the minute. In this sense, individuals' privacy has become an important issue for legislators around the world. It is essential to find the balance between (1) the respect for privacy, inviolability of personal information, the preservation and free development of personality and (2) the need for economic, social and technological development, and the importance of innovation.

1 Fabio Alonso Vieira is a founding partner and Carolina Barbosa Cunha Costa is an associate at Kestener, Granja & Vieira Advogados.

2 Tofler, Alvin, *A Terceira Onda*, 31ª ed. São Paulo: Record, 2012.

© Law Business Research 2020

Issues relating to data privacy and protection have been discussed in Europe and the United States since the 20th century. In Brazil, however, those discussions did not begin until 2010. Other Latin American countries, such as Mexico, are now putting in place their own privacy laws. Therefore, despite living in the information age and a digital world, nations and healthcare companies face (and will face) challenges related to regulating and setting forth best practices in privacy and data protection.

Privacy background in the European Union, United States and Brazil

The United States privacy experience

In 1890, Samuel Warren and Louis Brandeis published an article – 'The Right to Privacy' – in the *Harvard Law Review*, which structured the concept of privacy as 'the right to be let alone'. In the United States, the definition of privacy consists of 'the desire of people to freely choose the circumstances and the degree to which individuals will expose their attitude and behavior to others'.[3]

Based on this notion, the United States has divided its privacy concept into four categories: (1) information privacy, which is focused on establishing rules that govern the collection and handling of personal information; (2) bodily privacy, which is focused on an individual's physical being and any invasion thereof; (3) territorial privacy, which is focused on placing limits on the ability to intrude into another individual's environment; and (4) communication privacy, which encompasses the protection of the means of correspondence.[4]

As the US legal framework is structured on the federal system, each state has its own set of laws, rules and regulations regarding privacy issues. Typically, these laws, rules and regulations aim to provide the requirements for safeguarding data, disposal of data, data breach notifications and privacy policies.

In particular for healthcare, the US Health Insurance Portability and Accountability Act (HIPAA), enacted in 1996, is a federal act to govern privacy and security of healthcare information relating to health. This is analysed further later in the chapter (see 'Data protection specific to the healthcare sector in the United States').

The European experience

In 1970, within the individual state legal frameworks in Europe, there were already some rules aimed at protecting an individual's personal information, such as laws on privacy, tort, secrecy and confidentiality. However, owing to the increase in use of computers to process information about individuals and cross-border trade, facilitated by the formation of the European Economic Community, there was a need for new standards that allowed individuals to exercise control over their personal information.

3 Westin, Alan F, *Privacy and Freedom* (New York: Atheneum, 1967).

4 Banisar, David; Davies, Simon, 'Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection and Surveillance Laws and Developments', *John Marshall Journal of Computer and Information Law*, Vol. 18 (Autumn 1999) <https://papers.ssrn.com/sol13/papers.cfm?abstracts_id=2138799> (last accessed 8 February 2020).

© Law Business Research 2020

In the European Union (EU), the right to a private life and associated freedoms are considered as fundamental rights. Containing specific provisions relating to the right to privacy and family life and freedom of expression, the Universal Declaration of Human Rights was a starting point for framing standards for the protection of individuals. The principles set forth therein have provided the basis for subsequent European data protection law and standards.

In 1995, Directive 95/46/EC was enacted by the EU with the purpose of creating a set of rules for its Member States on the protection of individuals with regard to the processing of personal data and on the free movement of that data between Member States.

From 1995 to 2016, a series of regulations and rules were issued by the EU regarding privacy and data protection matters. Most recently, the General Data Protection Regulation (GDPR), a more rigid regulation on data protection, entered into force in 2018.

The Brazilian experience

Prior to Law No. 13709 of 2018 (LGPD), Brazil did not have any unique legislation relating to data protection, but a series of sparse laws to deal with privacy.

Only in 2010, a public debate to discuss privacy and data protection was launched by the authorities. This resulted in the draft of two bills that aimed to ensure and protect, within the scope of the processing of personal data, the dignity and fundamental rights of the natural person, and to ensure freedom, privacy, intimacy, honour and image rights.

In early 2018, with the *Cambridge Analytica* scandal and the entering into force of the GDPR, the Brazilian Congress approved urgent requests for analysis of the data protection and privacy bills.

On 14 August 2018, the LGPD was enacted. In the same year, other rules relating to privacy were also approved: (1) Decree No. 9637 of 2018, which set forth the National Information Security Policy; (2) Law No. 13787 of 2018 relating to computerised systems for the storage of patient records; and (3) Provisional Measure No. 869 of 2018, which modified certain provisions of the LGPD, created the National Data Protection Authority in Brazil (ANPD) and postponed the entry into force of the LGPD for 180 days.

It is important to note that there are more than 35 legal provisions addressing data protection issues scattered through the legal framework in Brazil, such as the Consumer Protection Code, the Telecommunications General Law, the Internet Civil Framework and the Access to Information Law. Furthermore, related specifically to health, Brazil follows the national Charter of Rights of Health Users and Code of Medical Ethics, the ANVISA[5] Resolution on Clinical Trials, pharmacovigilance and patient programmes, good pharmacy practices and a code of conduct for the pharmaceutical sector (Interfarma).

Data

The definition of 'data' is, and should be, generic. In some cases, it is difficult to define, mainly because of the constant technological advances and the dynamism with which the digital world evolves daily.

5 Agência Nacional de Vigilância Sanitária.

© Law Business Research 2020

'Data', in the context of computer science, refers to different pieces of digital information. Data are usually formatted in a specific way but can exist in different formats, such as numbers, letters, etc. When used in a media transmission context, 'data' refers to information in a binary digital format. In computing, the term is used broadly, but it is often used to identify and separate different pieces of information.

Raymond Wacks defines data as 'acts or signs that require interpretation before they acquire any meaning, remaining in the state of pre-information until they can be understood by someone'.[6]

Based on the foregoing, it is possible to conclude that data is information, such as numbers, images, texts, documents, in electronic, analogue, digital or non-electronic format, which, after scrutiny, have some meaning.

European and Brazilian law have divided the concept of data into four categories: (1) personal data; (2) sensitive personal data; (3) pseudonymised data; and (4) anonymised data. However, the United States divides the concept of data into just two categories: (1) personal information; and (2) non-personal information.

Personal data and personal information

Article 4(1) of the GDPR defines personal data as 'any information related to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier'.

In Brazil, Decree No. 8771 of 2016 defines personal data as 'data related to an identified or identifiable natural personal, including identification numbers, location data or electronic identifies, when these are related to a person'.

The LGPD maintained broad criteria to define personal data as 'any information related to an identified or identifiable natural person'.

The concept of personal data is central to data protection law. Since 1995, it is clear that the definition of personal data has been intentionally broad and, in theory, encompasses any and all information relating to an identified or identifiable natural person. This has created some challenges of interpretation as technology has evolved.

For this reason, in 2007, the Article 29 Working Party (under Directive 95/46/CE) prepared Opinion 4/2007 with the objective of reaching a common understanding about the concept of personal data, based on four building blocks: (1) any information (2) related to (3) any identified or identifiable and (4) natural person.

The expression 'any information' indicates the legislator's intention to provide for a broad concept of personal data and should be viewed based on the nature of the information, its content and format. Based on the nature of the information, the definition of personal data includes any type of statement about a person, regardless of whether the information is true or verifiable. From a content perspective, the definition should include data that provide any type of information (i.e., that reach private and family life). Last, the concept of data includes information available in any form (alphabetical, numerical,

6 Wacks, Raymond, 'Personal Information', *Privacy and the Law*, Oxford: Clarendon Press, 1989, p. 25.

© Law Business Research 2020

graphic, photographic and information stored, for example, in the memory of a computer in computer binary code format).

Information can be considered 'related to' when it refers to a person based on the elements of 'content', 'purpose' or 'result'.

- The 'content' element is present when information is given about a specific person, regardless of the controller's objective or the effect of that information on the person concerned.
- The 'purpose' element exists when the data is used for the purpose of evaluating, treating in a certain way or influencing a person's status or behaviour.
- The 'result' element determines the effect on an individual's rights and interests, which also takes into account that one person may be treated differently from another person as a result of the processing of certain data.

These three elements must be considered as an alternative and not a cumulative condition; this means that when the 'content' element is present, it is not necessary for the other elements to be present.

The expression 'identified or identifiable' establishes that a person can be considered 'identified' when, in a group of people, he or she is 'distinguished' from all others. Furthermore, a person is considered 'identifiable' when, although the person has not yet been identified, it is possible to do so.

The fourth expression, 'natural person' seeks to protect the personal data and rights related to a living human being, not being restricted to nationals or residents of a certain country.

The GDPR aims to protect and regulate only the use of personal data and to provide appropriate responses to rapid technological advances and globalisation issues that have caused a new level of collection, sharing and international transfers of personal data.

In the United States, the definition of personal information, or personally identifiable information, consists of any information that makes it possible to identify an individual, which includes social security number, passport number, an address, telephone number or email address. The definition generally applies to both electronic and paper records.

Sensitive personal data and sensitive personal information

Sensitive personal data are specific types of personal data, as they necessarily need to be connected to an identified or identifiable natural person. These types of data are subject to extraordinary protection, as they touch on an individual's privacy, and may subject an individual to discrimination or disregard. This means that these types of data have a greater potential to cause offence to an individual's fundamental rights.

According to Article 9(1) of the GDPR, the personal data that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, union membership, and the processing of personal data related to health and sexual life, require specific protection.

During the legislative process for the LGPD, the notions of which data would be considered sensitive and how these types of data would be processed were widely discussed. Contrary to the GDPR, the LGPD outlines sensitive personal data as data on 'racial or ethnic

© Law Business Research 2020

origin, religious and philosophical beliefs, political opinion, union membership, data related to health or sexual life, genetic or biometric data when linked to a natural person'.[7]

In the United States, 'sensitive personal information' is also an important subset of personal information. The definition of what is considered sensitive data varies depending on the jurisdiction and on particular regulations; for example, social security numbers, driving licence numbers, financial, medical and health information are usually treated as sensitive personal information. This type of information requires additional privacy and security limitations to safeguard it during processing (collection, use and disclosure).

Pseudonymised data

According to Article 4(5) of the GDPR, pseudonymisation is the process that occurs when personal data are processed in a manner that no longer can be linked to an individual without requiring additional information, provided that this supplementary information is kept separately and subject to technical and organisational measures.

According to Article 29 Working Group Opinion No. 5/2014, the most widely used pseudonymisation techniques are (1) encryption with a secret key, (2) hash function, (3) hash function encoded with a key and (4) use of authentication devices (tokens).

The LGPD defines the pseudonymisation process as 'the processing through which the data loses the possibility of direct or indirect association with an individual, if not through the use of additional information maintained separately by the controller in a controlled and secure environment'.[8]

In US law, pseudonymised data exists when information about an individual is retained under pseudonyms, such as a unique numerical code for each person, that renders data temporarily non-personal. This reversibility can be reversed, re-identifying the individuals.

As pseudonymised data can be reversed, this measure is widely used by the pharmaceutical sector, for instance, in drug trials.

Anonymised data and non-personal information

'Anonymised data' is not personal data, as it does not relate to an identified or identifiable natural person; this means, that the identification or re-identification of the data subject is impossible, by any part and through the use of any reasonable means. Therefore, in order to be classified as 'anonymised data', the data must be stripped of any identifiable information, making it impossible to derive any of the data subject's information, even by the person that was responsible for performing the anonymisation techniques.

According to Article 29 Working Group Opinion No. 5/2014, (1) the true anonymisation of data is an extremely high barrier to be reached; (2) data controllers often fall short in effectively anonymising data; (3) anonymisation techniques can guarantee privacy, but only if their application is properly engineered, with prerequisites (context) and the objectives of the anonymisation process clearly set out, in order to achieve the anonymisation purposes, while producing useful data; (4) the ideal solution must be decided in each case,

7 Law No. 13709 of 2018 (General Law on Protection of Personal Data) [LGPD], Article 5º, Paragraph II.

8 LGPD, Article 13, § 4º.

© Law Business Research 2020

possibly using a combination of different techniques, and always taking into account that a set of anonymised data may still present risks to its data holder; and (5) anonymity and its risks must be regularly reassessed by the controllers.

Opinion No. 5/2014 also provides two anonymisation techniques: (1) randomisation, which aims to change the veracity of the data to remove the strong link between the data, the data subject and the data holders; and (2) generalisation, which aims to generalise or dilute the attributes of the data subjects by modifying the scale or the order of magnitude.

It is emphasised that a set of 'anonymised data' can present residual risks for the data holders, because even when it is no longer possible to accurately recover an individual's records, other available sources, public or not, can be used.

US law determines that if the data elements used to identify an individual are removed, the remaining data becomes non-personal information, and privacy and data protection laws generally do not apply in these cases.

'Anonymised data' is frequently used for research, statistical or aggregated purposes.

Data processing

The definition of personal data processing provided by Article 4(2) of the GDPR is extremely broad, as it includes any operation or set of operations carried out on personal data, with or without automated means, which encompasses all processes from the collection to the destruction of the personal data.

Furthermore, personal data processing is only allowed if at least one of the hypotheses as provided in Articles 6(1) or 9(2) of the GDPR is present. These include (1) when the data subject has given consent to the processing of his or her personal data for one or more specific purposes, (2) for compliance with a legal obligation to which the controller is subject, (3) to protect the vital interests of the data subject or of another natural person and (4) for the purposes of legitimate interest.

The LGPD, when defining processing, also sought to understand the entire data life cycle, which includes collection, reception, access, transmission, processing, storing and controlling the information, modifying, communicating, transferring, or the process of extracting or eliminating.

In theory, the processing of personal data consists of the application of methods and database tools that cover the entire processing operation or set of processing operations, carried out with or without the aid of automated means, ranging from the collection to the elimination of data.

Thus, as in the GDPR, the LGPD establishes the hypotheses for the processing of personal data (in Article 7) and of sensitive personal data (in Article 11). These include, for example, (1) when the data subject has provided consent to fulfil a legal or regulatory obligation, (2) to carry out studies by research bodies, (3) for the protection of life or the physical safety of the data subject or a third party, (4) for the protection of health in a procedure carried out by a health profession or by a health entity, and (5) when necessary to serve the controller's legitimate interest.

In the United States, privacy and data protection laws, which vary from state to state, usually define processing as essentially anything someone may do with personal

© Law Business Research 2020

information, such as collection, recording, organisation, storage, updating, modification, retrieval, consultation, use, disclosure, linking, alignment or combination, blocking, erasure or destruction.

Data protection in the healthcare sector

General aspects

Special privacy protections for healthcare date back thousands of years. The modern Hippocratic Oath states: 'I will respect the privacy of my patients, for their problems are not disclosed to me that the world may know.'[9]

There are many reasons why privacy rules are generally stricter when related to health and healthcare issues. First, medical information concerns the inner workings of an individual's body or mind. The individual's sense of privacy may be violated if others have unlimited access to this type of information. Second, it is a belief that patients will be more open about their medical conditions if they have the certainty that any potentially embarrassing medical facts or information will not be revealed to unauthorised third parties. Third, medical privacy protections avoid discriminatory situations.

Even though there are strict laws protecting health and medical information within the industry, modern insurance, healthcare and pharmaceutical companies and medical practices often use patient information extensively. For instance, researchers may use medical information, such as that processed during a clinical trial, to find new patterns as they seek to develop cures for illnesses and promote public health. Also, healthcare providers may use patient records to evaluate their overall quality of care.

As mentioned previously, the aim of data protection principles is to protect an individual's privacy, confidentiality and free development of personality. However, one cannot focus exclusively on the individual's privacy and forget the need to promote innovation and social and technological developments, in particular those related to developing cures for illnesses and promoting public health.

Data protection specific to the healthcare sector in the United States

As already mentioned, HIPAA is the US federal act that governs privacy and security of healthcare information relating to healthcare providers, including doctors' medical practices and hospitals, health plans and health insurers, and healthcare clearing houses, such as third-party organisations that host, handle or process medical information. In view of the federal system in the United States, each state may enact its own laws to deal with privacy in the healthcare sector.

HIPAA provides two important definitions related to healthcare information:

- protected health information (PHI), which:
  - is any individually identifiable health information that is transmitted or maintained in any form or way;
  - is held by a covered entity or its business associates;

9 Tyson, Peter, 'The Hippocratic Oath: Modern Version', WGBH Educational Foundation, 2001 <www.pbs.org/wgbh/nova/body/hippocratic-oath-today.html> (last accessed 8 February 2020).

© Law Business Research 2020

  - identifies the individual or offers a reasonable basis for identification;
  - is created or received by a covered entity or an employer; or
  - is related to a past, present or future physical or mental condition, provision of healthcare or payment for an individual's healthcare; and
- electronic protected health information (ePHI) is any PHI that is transmitted or maintained in electronic media, for example, computer hard drives, magnetic tapes or disks, or digital memory cards. Paper records, paper-to-paper and fax transmissions are not considered transmissions via electronic media.

Compared with other US privacy laws, HIPAA provides perhaps the most detailed implementation of the 'fair information practice principles', as it includes requirements concerning privacy notices, authorisations for use and disclosure of PHI, limits on use and disclosure to the minimum necessary, individual access and accounting rights, security safeguards and accountability through administrative requirements and enforcement.

As the objective of the PHI is to improve the efficiency of the healthcare system, HIPAA does not require from covered entities the need for authorisation granted by individuals for certain categories of medical treatment, payments and surgeries. Further, it does not apply to medical research and de-identified information, which means that if the information does not actually identify an individual and if there is no reasonable basis to believe that the information can be used to identify an individual, HIPAA does not apply.

Additionally, HIPAA also provides minimum security requirements for PHI, with the objective of ensuring that covered entities adopt procedures to prevent, detect and correct security violations, such as (1) ensuring the confidentiality, integrity and availability of all ePHI that a covered entity creates, receives, maintains or transmits, (2) protecting against any reasonably anticipated threats or hazards to the security or integrity of the ePHI, (3) protecting against any reasonably anticipated uses or disclosures of information that are not permitted or required under privacy rules, and (4) ensuring compliance with the security rules by its workforce.

In the development of a related compliance programme, each covered entity must observe the following factors:

- the covered entity's size, complexity and capabilities;
- its technical infrastructure, hardware and software security capabilities;
- the costs of security measures;
- the probability of potential risks to electronic protected health information;
- identification of an individual who is responsible for implementation and oversight of the compliance programme;
- initial and continuing risk assessments to identify potential risks and vulnerabilities, each of which must be addressed; and
- a security awareness and training programme for its workforce.[10]

10 Security Standards General Rule, §164.306 (b) (2) <https://www.govinfo.gov/content/pkg/CFR-2004-title45-vol1/pdf/CFR-2004-title45-vol1-sec164-306.pdf>.

© Law Business Research 2020

It is important to point out that HIPAA does not pre-empt state laws that provide more protection than federal law.

This may be one of the most sensitive issues in relation to the processing of an individual's data in the United States. Each state may enact different rules, some being more strict than others. This situation may allow certain covered entities to move from one state to another, pursuing more flexible rules that may benefit its activities and business. Also, considering the data fluidity between entities across the states and the world, this situation may create an insecure environment for those parties who process data in the United States, whether in the healthcare sector or any other.

Alongside HIPAA, the US health legal framework also contemplates (1) the Health Information Technology for Economic and Clinical Health Act (HITECH), which governs the adoption and meaningful use of health information technology (HITECH strengthened HIPAA to address the privacy impacts of the extended use of electronic health records); (2) the Genetic Information Nondiscrimination Act of 2008 (GINA), which sets forth limits on the use of genetic information in health insurance and employment; and (3) the 21st Century Cures Act of 2016 (the Cures Act), which has the purpose of expediting the research process for new medical devices and prescription drugs, speeding up the process for drug approval and reforming mental health treatment.

GINA prohibits health insurance companies from discrimination based on genetic predispositions in the absence of manifest symptoms or from requesting that applicants receive genetic testing, and prohibits employers from using genetic information in making employment decisions.

The Cures Act provides the following privacy provisions:

- certain individual biomedical research information exempted from disclosure under the Freedom of Information Act;
- researchers permitted to review PHI remotely;
- certificates of confidentiality for researchers; and
- compassionate sharing of mental health or substance abuse information with family members or carers.

Data protection specific to the healthcare sector in the European Union

The GDPR presents challenges for all industries and sectors of the economy, in particular for the healthcare sector as it considers data concerning health as a special category of data and provides a specific definition for health data.

As set forth in the GDPR, 'data concerning health' is defined as 'personal data related to the physical or mental health of a natural person . . . which reveal information about his or her health status'; 'genetic data' is understood as 'personal data relating to inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question' and 'biometric data' as 'personal data resulting from specific technical processing relating to the physical,

© Law Business Research 2020

physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person'.[11]

The GDPR aims to ensure that the data subject has the fundamental right to the protection of his or her health data in numerous situations, such as a cross-border healthcare context and in medical research, such as clinical trials, clinical investigations, epidemiological research and patient registry.

Consequently, healthcare organisations that typically manage health data, such as hospitals and medical practices, have the additional burden of maintaining data concerning health, genetic data and biometric data to a higher standard of protection than personal data in general.

Additionally, processes that foster innovation and better-quality healthcare, such as clinical trials or mobile health, need robust data protection safeguards to maintain the trust and confidence of individuals in the rules designed to protect their data.

To provide safeguards for these innovations and better-quality healthcare, during the past year, the European Data Protection Board (EDPB) has issued opinions on the following matters: (1) 'EDPB-EDPS (European Data Protection Supervisor) Joint Opinion 1/2019 on the processing of patients' data and the role of the European Commission within the eHealth Digital Service Infrastructure (eHDSI)' (Opinion 1/2019);[12] and (2) 'Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulations (CTR) and the General Data Protection regulation (GDPR)' (Opinion 3/2019).[13]

The eHealth Network provided in Opinion 1/2019 is a voluntary electronic network of responsible authorities for eHealth designated by Member States. The eHealth Network is an initiative to preserve and protect patients' rights in cross-border healthcare and to enhance interoperability between national digital health systems in exchanging patients' data contained in ePrescriptions, Patient Summaries and electronic health records. The Commission has also developed an IT tool, namely the eHealth Digital Service Infrastructure for the exchange of health data. These are all measures to keep up with the dynamic exchange of data and innovation in accordance with the principles set forth in the GDPR.

Opinion 3/2019 provides specific guidelines for the processing of personal data in the course of a clinical trial protocol. The EDPB in this case considered it relevant to distinguish between two main categories of processing activities: (1) the processing operations purely related to research activities; and (2) the processing operations related to the purposes of protection of health, while setting standards of quality and safety for medicinal products by generating reliable and robust data (reliability and safety purposes). In both cases, the conclusion is that the controller and the processor would process data for those purposes on the grounds of public interest, legitimate interest or, if necessary, with the explicit consent of the patient.

11 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Article 4 (Definitions), Paragraphs 13, 14 and 15.

12 Available at https://edps.europa.eu/sites/edp/files/publication/19-07-15_edpb_edps_joint_opinion_ehealth_en.pdf.

13 Available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinionctrq_a_final_en.pdf.

© Law Business Research 2020

Data protection specific to the healthcare sector in Brazil

Health is a fundamental right in Brazil, established in the Federal Constitution and regulated by Law No. 8080 of 1990, as amended. Law No. 8080 sets forth principles related to the rendering of public and private healthcare services, such as:

- universal access to health services at all levels of assistance;
- comprehensive care, understood as an articulated and continuous set of preventive actions and services;
- preservation of people's autonomy in the defence of their physical and moral integrity;
- equality of healthcare, without prejudice or privileges of any kind;
- right to information regarding healthcare; and
- disclosure of information regarding healthcare services.

As the LGPD is not in force yet and the ANPD has not been incorporated, currently there is no specific data protection legislation or opinion when processing health data. It is also not clear what kind of activities or situations would fall under the terms 'protection of life' or 'the physical safety of the data subject or of third parties and for the protection of health' as set forth by the LGPD, in a procedure performed by healthcare professions or by healthcare entities. In other words, it is not entirely clear what is the extent of the definition of these terminologies for the LGPD and for the ANPD.

Despite not having a specific legal framework for data protection and privacy matters related to health data, there are legal provisions scattered in the Brazilian legal framework that address confidentiality issues relating to healthcare information that includes personal information; for example, the Consumer Protection Code, the Charter of Rights of Health Users, the Code of Medical Ethics, Good Pharmacy Practices, ANVISA Resolution No. 9 of 2015 on Clinical Trails and the Code of Conduct for the pharmaceutical sector (Interfarma).

From a Brazilian law perspective, the concept of confidentiality is different from privacy. Confidentiality means that the information disclosed by one party to another shall not be made publicly available to any third party. Confidentiality provisions usually do not provide the necessary safeguards or protections for the processing of data.

When the LGPD comes into force, these legal provisions shall also remain in force. Bearing in mind that there is a complex and intense flow of data in respect of health matters, for example, in clinical trials, there are various parties, such as the sponsor, the researcher and his or her medical team and the research facility, each of whom has access to different levels of personal and sensitive personal data. This means that, in particular, for health information, it will be necessary to perform case-by-case analysis and assessments in respect of privacy and data protection matters.

The protection of life and the physical safety of the data subject or of third parties and for the protection of health, in theory, are not applicable to the main activities performed by the pharmaceutical industry, which, generally, consists of manufacturing and distributing drugs and medical devices. This does not mean, however, that the support activities developed by the industry, such as patient programmes, do not fall into this category. Therefore,

© Law Business Research 2020

the challenge for Brazilian data protection professionals is to analyse and assess these activities case by case and to check whether they fall under the definitions of the LGPD.

During the past year, Brazil has had a few data breaches involving health data: 2.4 million users of the healthcare system, SUS, had their data exposed on the internet; and the healthcare insurance company, Unimed, had its whole data bank linked. These breaches highlight the need for investment in data privacy compliance programmes, to respond quickly and mitigate liabilities, as well as security and infrastructure measures.

Once the LGPD comes into force, these data breaches shall be subject to penalties that range from warnings issued by the ANPD, with a deadline for the adoption of corrective measures, a fine of up to 2 per cent of the sales revenue of the legal entity of private law, group or conglomerate in Brazil in the previous fiscal year, excluding taxes (limited, in the aggregate, to 50 million reais per infraction), to a partial or total ban on the processing of personal data and all related activities.

Conclusion

We live in a digital environment filled with several types of artificial intelligence and highly sophisticated electronic devices, all of which assist in the development of global society. This situation brings enormous advantages to mankind, in particular in the health sector with the development of treatments, examinations and new drugs that expand our quality of life and life expectancy, among other things.

In this sense, the first challenge is to find a balance between preserving an individual's privacy, inviolability of confidentiality and free development of personality, and not hampering the development of new technologies and innovative initiatives.

As data is fluid, abstract and can easily be transferred from one side of the world to the other, another challenge, in particular for the healthcare industry, involves guaranteeing that all the parties to the same data chain are processing the data in accordance with one or more data protection laws. It seems that the security measures available and the structure for the protection of data are insufficient for the nature of the activities that have been developed by humanity. It is important to consider creating new tools that would make it possible for the data subject to maintain control over the processing of his or her own data by third parties, controllers and processors.

Taking into account the enormous amount of data that is transferred between different countries, we face the challenge of harmonising the understanding of privacy and data protection matters in order to contribute to data protection programmes. Also, it is fundamental to create a definitive understanding of privacy and data protection for controllers and processors headquartered in multiple jurisdictions.

In this context, the federalist system of the United States and the deviation mechanism set forth by the GDPR may bring some kind of interpretation conflict or insecurity in connection with this matter.

It is clear that the world has advanced a lot in respect of data privacy and protection issues, but the time has not yet come to stop those advances or consider that an individual's privacy will always be safe and protected.

© Law Business Research 2020

Appendix 1

About the Authors

Fabio Alonso Vieira

Kestener, Granja & Vieira Advogados

Fabio Alonso Vieira is a founding partner and head of innovations, technology, data protection and privacy. Passionate about challenges, it has become clear that with innovation, technology and the speed at which things are evolving, the industrial world as we know it will not exist in the future. Therefore, Fabio has been tackling face on the challenges relating to data protection and privacy for companies in the pharmaceutical, food, cosmetics, information technology and internet sectors, being a versatile lawyer with a strong academic background. Fabio graduated from the Mackenzie University in 1998. He has a specialisation in contracts (2001) and a master's degree and PhD in international law (2014-2015), all from the Pontifical Catholic University of São Paulo.

Carolina Barbosa Cunha Costa

Kestener, Granja & Vieira Advogados

Carolina Barbosa Cunha Costa graduated from the Pontifical Catholic University of São Paulo and is an associate who advises domestic and international clients on innovations, technology, data protection and privacy. Carolina has worked actively and been directly involved in significant transactions and projects for companies in the pharmaceutical, food, cosmetics, information technology and internet sectors. She has specialisations in startups and innovation (2017) and data protection and privacy (2018) both from INSPER. She has published articles on data protection, privacy and innovation in reputable publications in Brazil, such as *Valor Econômico* and *Revista de Direito das Startups*.

© Law Business Research 2020

Kestener, Granja & Vieira Advogados
Rua Funchal, 418
Vila Olimpia
São Paulo 04551-060
Brazil
Tel: +55 11 3149 6100
fabio.vieira@kgvlaw.com.br
carolina.costa@kgvlaw.com.br
www.kgvlaw.com.br

© Law Business Research 2020

Published by Latin Lawyer and LACCA, edited by Andrew M Levine, a litigation partner at Debevoise & Plimpton LLP, Reynaldo Manzanarez Radilla, a corporate attorney and compliance professional, Valeria Plastino, vice president, general counsel and regional ethics and compliance officer at CenturyLink, and Fabio Selhorst, general counsel, chief integrity officer and chief communications officer at Camargo Corrêa Infra, *The Guide to Corporate Compliance* is designed to assist key corporate decision makers and their advisers in the effective handling of their compliance obligations in Latin America.

The guide delivers specialist insight to our readers – general counsel, compliance officers, government agencies and private practitioners – who must navigate the region's complex, fast-changing framework of rules and regulations.

In preparing this guide, we have been working with practitioners from a variety of disciplines and geographies, who have contributed a wealth of knowledge and experience. We are grateful for their cooperation and insight.

Visit latinlawyer.com
Follow @Latin_Lawyer on Twitter
Find us on LinkedIn

an LBR business

ISBN 978-1-83862-428-6

© Law Business Research 2020