PERSONAL DATA IN THE SOCIAL SECURITY INSTITUTE: EXPLORATORY ANALYSIS ON SOME PERSONAL DATA PROTECTION PRACTICES IN THE SOCIAL SECURITY SYSTEM OF THE PARAGUAYAN STATE

Submitted: 05/12/2019
Revised: 15/01/2020
Accepted: 08/03/2020

Article submitted to peer blind review

Eduardo Carrillo[*]
Maricarmen Sequera[**]

DOI: https://doi.org/10.26512/lstr.v12i2.34689

Abstract

Purpose – The research aims to observe and describe the legal framework and implementation practices of personal databases management in the Social Security Institute (IPS), the most important public social insurance system in Paraguay.

Methodology – The research is exploratory, consisting on both substantive and procedural law analysis of health information storage regulations and its compliance. Also, interview to private companies, the public sector and one qualified worker insured by IPS are conducted to better understand collection, storage and maintenance of health records databases.

Findings – Research indicates evidence that biometric data storage of insurers does not have adequate regulation for its protection. It also shows evidence that private companies don't deliver by default medical records to workers, as well as potential access to these records by administrative personal. Evidence also signals that clinics performing medical examinations request more sensitive information than required by law. Research limitations It is identified that a broader private company sample could be of use to better understand workers health record collection. Also, third party auditing IPS IT systems could be of use to further understand information management practices and vulnerabilities.

[*] Carrillo in an international affairs graduate interested in the intersection of digital rights and TLGBQI communities. He has conducted research on city security with technology and personal data protection in the public and private sectors. He previously worked on the "Who Do We Choose" project and the International Organization for Migration. E-mail: educarrillo90@gmail.com.

[**] Sequera is the co-founder of TEDIC. She works in the area of public policies and directs digital rights projects in the organization. Researcher in Human Rights and Technology. Lawyer of the National University of Asunción. She has several publications on Cybersecurity, Privacy, Freedom of Expression and Gender on the Internet. E-mail: maricarmen@tedic.org.

Practical Implications – A series of discretional practices are identified, signaling regulatory standardization urgency for all actors. A comprehensive Protection of Personal Data Act is needed.
Originality – No comprehensive research targeting the IPS system and its health personal data management processes is identified. The research is considered an initial contribution to the state of the art on the subject and specially to biometric collection and storage.

Keywords: Privacy. Personal Data. Sensitive Data. Biometrics and Health Data. Social Security.

INTRODUCTION

There is a historical need to reform and update the current legislation on the protection of personal data in Paraguay[1]. There is currently a gap between the progress of the information society, with the management of personal data by authorities and institutions, both in the public and private sectors.

In regard to the health field in its broad sense, there are still several fronts that need to be explored from a personal data protection approach and linked to the ethical limits demarcated by the legal regulations, the practice or exercise of medical secrecy, as well as international standards.

The present research arose from the complaint of an anonymous worker who came to the TEDIC organization to inform about contrary and invasive practices to the privacy of the workers, within the framework of the application of the admission and annual medical examination that workers in Paraguay must take. According to his testimony:

> "They left the form on the desk of each staff member, and each one filled in and then by group they went to a private laboratory so they could take the samples. […] The company that asked for the medical examinations was the one that distributed the forms. It was a well-known clinical laboratory."

Specifically, this form included a series of highly invasive questions. It should be remembered that occupational medical examinations only seek to determine the fitness of a worker with respect to the assignment he or she already performs or will perform.

In the case of working women, there was a specific section with gynecological questions and included very specific questions. These questions

[1] Nowadays, Act no. 1628/01 is currently in force in the country and it regulates private information together with its amendment, Act N°1969/02. More Information in: https://bit.ly/3mobQmT.

aimed at collecting data that had nothing to do with the proper exercise of a job responsibility, for example, if a worker had a clinical abortion:

Questions for Women Only:
Has Had Breast Swelling Yes – No
Suppuration or Blood in the Nipple Yes – No
Breast Surgery Yes – No
Pain During Menstruation Yes – No
Hot Flashes Yes – No
Spontaneous Pregnancy Loss Yes – No
Pregnancy Loss (Clinical Reason) Yes – No
Date of Last Menstruation

Thus, a new concern arises regarding the discretion and freedom with which the questions of this form were prepared and subsequently applied to workers in their places of work.

According to the worker interviewed, this questionnaire was applied in at least one more company which performs similar functions as his. In the case of the company in which he worked; the workers refused to fill in this form as it was an invasion of privacy and an exercise in resistance was done.

On the other hand, there is the regulation of fingerprint collection of insured persons of IPS, which was approved in 2015 and applies to people from 2 years old on. This resolution arises from **complaints of corruption** in the state social insurance by companies and insured persons and to prevent the theft of medications in such institution.

The resolution only talks about the importance of the implementation of the system as a tool for digitalization and optimization of the institutional management but without an analysis of the impact of the collection of sensitive data of the insured persons.

In all the above, risks and abuses are identified by various actors involved in the process of collection and systematization of personal data that needs to be explored from different approaches. In this way, it is sought to understand not only the reasons that lead to this collection, but also to identify potential practices that would put at risk the human rights of workers, which could end up in situations of discrimination, violation of privacy and abuse of power.

OBJECTIVES OF THE RESEARCH

The objective of this research is to describe the legal situation regarding the management of personal databases in the Paraguayan public health system.

In order to comply with the general objective of the study, the local context is identified about the uses, management and procedures, as well as current

national legal regulations that define the implementation of the storage of sensitive health information in the Social Security Institute. On the other hand, interviews are held with those in charge of the storage system for health sensitive information of IPS to investigate which principles, protocols and standards they use for the protection of health data.

METHODOLOGICAL STRATEGY

The research has an exploratory approach. Also, an analysis of substantive and procedural law that is closely related to the use of information technologies will be conducted. It is intended to know the current status and the challenges for the implementation of regulations that regulate the storage of sensitive information on health issues, as well as the compliance or not of standards of personal data protection and other human rights.

In this regard, **two methodological tools** will be used: first, the **legal analysis** of the current regulations of the Social Security Institute that will serve to make a diagnosis for the process of their implementation. It will be contemplated with the development of a conceptual framework of personal data to measure the current legal application. In the second part of the research, **semi-structured interviews** will be conducted to determine the status of implementation of regulations for the storage of sensitive health data. The sampling frame was constructed by selecting actors from the private sector (companies), as well as people insured in IPS and a responsible person involved in the storage of sensitive health data in IPS.

These interviews seek to inquire about the quality and the status of application of IPS regulations and public international law in matters of health, privacy and confidentiality of health data. Using this approach will serve as a tool to strengthen the normative framework, as well as to identify its limitations and challenges of the IPS health system.

SAMPLING FRAME

A grand total of seven interviews were conducted: four from the private sector, two from the public sector and one worker as a qualified informant. Even though the public sector agreed to the interview, they did not respond to the consultation made through the access to public information website.

RESOLUTIONS OF THE SOCIAL SECURITY INSTITUTE - IPS

Biometric Data for Access to State Social Insurance

If you use this template, there will be no need to check the page size of your submission. With the argument of "you are looking for patient comfort and general security" when collecting medications, medical imaging and analysis, the Board of the Social Security Institute (IPS) approved in 2015 the biometric registration of all its insured persons, from 2 years of age. In 2016, the resolution of the Board of Directors of IPS No. 003-050/16 came into force, which obliges patients and patients' authorized persons to register their fingerprints in order to withdraw high-cost cancer medications. The Central Hospital pharmacy together with the Customer Service Center (CAU) implemented this mandatory procedure for the collection of medications, gradually extending to all IPS insured.

During the first months of 2016, fingerprints of 1,000 patients were registered for collections in external pharmacy. Gladys Coronel, head of the Department of Pharmacies, said that the goal for that year was to reach the 7,000 registered insured and 21,000 authorized persons (ABC Color, 2016).

In 2017, the IPS newsletter highlights the importance of enrollment to access the IPS health service (Communication Office of the Social Security Institute, 2017):

> "Enrolling means that at some point, instead of using the identity card, the fingerprint is used, when the patient puts their fingerprint, all their data is released, if he/she is up to date, if he/she is insured, which insurance corresponds, if prosthesis is applicable or not, etc. We seek for the patients' comfort and general safety, there is a certain process that now has to be done, checking the rights, going from one office to another, searching the computer system etc. All that will disappear by using just the fingerprint" (Dr. Manuel García, Medical Director of the Central Hospital).

The implementation of the IPS biometric system is not regulated in the Paraguayan national legislation. Although the right to privacy is recognized in the National Constitution of Paraguay (Art. 33), in practice there are not enough measures to guarantee compliance with this right, as evidenced by the processing of personal data in public and private databases (TEDIC, 2017).

Act no. 1682/2001 that regulates certain aspects of data processing in our country is far from complying with minimum standards of personal data protection, such as the self-determination of the data subject, the requirement of purpose of the collection, the storage time of the data, proportionality, data quality control, scope of application, accountability, among other principles. In addition, a great absence in this administrative resolution are the administrative sanctions

in case of abuses in the treatment of sensitive data and databases, by any public or private entity.

A research of ADC Digital on Biometrics and protection of personal data contemplates a case investigated by the University of North Carolina:

> "A research that has found significant differences between fingerprints belonging to people of African descent and people of European descent. Although researchers themselves state that a larger sample of people and a more diverse analysis of ethnic groups are necessary to obtain a definitive conclusion, the first scientific results indicate a high possibility that the fingerprints reflect specific patterns of a specific ethnic group" (FERREYRA, 2017).

As a result, the storage of fingerprints in Paraguay meets the conditions required to be classified as sensitive data. The resolution of the Administrative Board of IPS **does not include a previous analysis** to justify the implementation of this type of system. According to data processing standards, an impact evaluation is mandatory for the collection of **biometric data** based on the **principle of the need** to use this type of systems. Nor does it justify why the current identity card – issued by the State itself to identify citizens – does not serve as an identification tool to carry out the legal act before IPS. This mechanism would be less invasive than the collection of fingerprints, and therefore, the risk of violation of fundamental rights would be greatly reduced.

According to the newsletter that is mentioned at the beginning of this section, it is sought to avoid bad intentions of people when using the identity of third parties for criminal purposes. But to justify the collection of biometric data, which are sensitive data, it must be analyzed if there is no alternative way that affects to a lesser extent the rights of the people and, at the same time, can achieve the objectives that are pursued (EFF, 2016). This measure, that seeks to be preventive to avoid any type of crime, not only reflects a disproportion in terms of the aim pursued, but also leaves aside the ideal of a minimal intervention by the punitive apparatus of the State, typical of what is called "minimal criminal law".

The design of the system for the prevention and prosecution of crimes must take into account that it cannot end the criminal chain that it seeks to fight on its own. There are some alternatives that can be more effective and less invasive for people, such as the voluntary identity implantation report, the cooperation between operators, or the tracking and capture of criminal gangs dedicated to this illegal activity.

The former UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression and the UN High Commissioner for

Human Rights have expressed concern about violations of the right to privacy due to the lack of effective protection measures in the use of biometric technologies.

For his part, the former UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms in the Fight Against Terrorism determined in his report published in 2009 that, although the use of biometrics is presented in certain circumstances as a legitimate tool for the identification of suspects in cases of terrorism, there is a special concern about:

> "The cases in which biometrics is not stored in an identity document, but in a centralized database, increasing the risks for the security of the information and leaving individuals vulnerable. As biometric information increases, error rates can increase significantly" (UCCIFERRI, 2017)."

The increase in error rates can lead to the illegal criminalization of individuals or social exclusion. At the same time, the Rapporteur highlights an aspect that was mentioned earlier, the irrevocability of biometric data: "[...] once copied and/or fraudulently used by a malicious actor, it is not possible to issue an individual a new biometric signature (identity)."

It also highlights that biometric data present obstacles of privacy and confidentiality that at first glance seem to be overcome if the concept of confidentiality is redefined and readjusted: moving from an information confidentiality model based on trust, to an anonymous data model. That is, anonymization should be a basic requirement to build a biobank.

However, some authors (FARIA; CORDEIRO, 2014) consider that there are doubtful areas in the validity of this "guarantee". On one hand, they claim that the anonymization of data

> "often hides situations in which, in fact, there is still the possibility of re-identifying data, and therefore, that anonymity is not real or complete".

On the other hand, the strongest doubt is that the anonymity is used as a

> "rhetorical strategy to deny the existence of any subjective interest in human biological materials (HBM) and, consequently, to affirm its free availability for those who can do an interesting use of them, such as the medical and biotechnology industry".

Admission Medical Examination of IPS

There is a great number of Resolutions of the Board of Directors of IPS[2] concerning the payment of admission medical examination of the workers. All these resolutions are in line with the legal obligation of the Labor Code – Act no. 213/9. In this regard, Article 275 establishes the submission of workers to periodic examinations established by the employer, with no costs for the workers. Through this norm, IPS can request each employer the examinations of each worker in case of suspicion of insurance fraud or at the moment of registration in IPS.

Likewise, what is stated in Annex 1 - Admission Medical Examination of Resolution C.A no. 099-022/16, Numeral 7:

> Requirements. The medical-labor board may require the employer to submit other laboratory analyzes, imaging and medical examinations.

It is important to highlight that the rights interconnected to privacy and confidentiality with respect to medical information and medical history have been widely discussed in the fields of bioethics and health act. These have been the object of consensual and challenging ideas. It is indisputable that medical secrecy remains a key to medical work: even without this criterion most patients would not disclose part of their intimate medical history. It is therefore important to emphasize the notion that the right to confidentiality in health not only serves to preserve a significant element of trust, but also to prevent stigmatization and defense against discrimination. Therefore, measures to protect confidentiality are key to public health.

ANALYSIS OF INTERVIEWS

In order to understand the scenario surrounding the implementation of Resolution CA no. 099-022/16 of IPS, of the Board of Directors of IPS no. 003-050/16 on biometrics and other related topics[3], a series of interviews were conducted with State civil servants linked to such regulations and representatives of the private sector in different areas and linked to the management of personnel within the companies. The IPS Economic Performance Manager was interviewed from the public sector, under whose management is the Occupational Hazards and Subsidies Department, a unit within the IPS directly linked to the implementation of Resolution no. 099-022/16. The Director of the Department of Inspection and

[2] Resolution no. 099-022/16; Resolution no. 024-009-17; Resolution no. 090-022/17; Resolution no. 035-007/17.

[3] Management of data bases in general and the collection of biometric data for access to medicines by the Social Security Institute.

Supervision of the Ministry of Labor was also interviewed, a body that controls the documentation of the workers in the framework of the annual periodic examination.

In relation to the private sector, four companies of different categories were identified and with a minimum average of 150 employees. For all cases, both the admission and annual medical examination is an obligation that must be complied.

It should be noted that in order to improve the authenticity of responses, interviews were conducted with anonymity agreement, both with respect to the person and the company in which he/she works. An approximation and accurate understanding of the phenomenon addressed by the present research is sought.

To order the most significant information given by each of the sectors interviewed, there will be a differentiated disaggregation of the testimonies, starting the analysis of the interviews conducted with IPS and the Ministry of Labor, by the different nature of the questions asked to said entities of the State, to then go on to analyze the interviews to the different companies that agreed to the interviews.

Interviews with IPS Authorities

If you use this template, there will be no need to check the page size of your submission. In relation to the Social Security Institute (IPS) and the consultations of different nature and scope that were conducted, they show that the necessary and sufficient regulations that justify the collection of health data of workers in the framework of the Admission Medical Examination, are Article 275 of the Labor Code and Resolution C.A no. 099-022/13. The interviewees mentioned that, since 1993, admission-type examinations for workers were taken through consultations, but because of the institution's own capacity, this was very complex, so the current regulations that are more direct and easier to sustain were opted by IPS.

Regarding the safeguard criteria carried out by the Labor Registry and Subsidy Department, as well as the processes of loading and systematizing said information, the interviewee mentions that initially the organism had planned to receive the medical examinations, but this was subsequently modified by resolution, thus safeguarding the confidentiality of patients:

> "First, the admission exam was to be presented to IPS, but that was subsequently modified by resolution and became an Affidavit. What is informed to me? Worker X took the admission exam and is fit for work. If the doctor refers on the certificate, he/she can write: the patient has mild diabetes, congenital heart disease, and the doctor's information is included in the certificate. We do not receive medical examinations or anything. That is also

> why the confidentiality of patients is guaranteed. The information we receive is also allowed only to our medical professional personnel. Obviously, those who do face-to-face deliver the document in a window and an administrative officer uploads it online. But the REI[4] system is direct, not even we, the IPS administrative staff, see it. We are interested in knowing whether the person is fit or not, if refers X pathology or not. The issue of HIV was removed and is not part of the Admission Medical Examination. Tripartite meetings were held with HIV prevention organizations, the Ministry of Labor and we even issued joint statements. Because that was used to discriminate. People were detected and fired."

On the other hand, as regards the deletion of old data, and rectification mechanisms thereof, there is evidence of a lack of differentiation of the types of data that can be deleted without obstructing the nature and functioning of IPS in safeguarding the interest of workers. There are also no constant data update processes:

> "In general, IPS does not delete information. Because it is linked to very long-term benefits. If in 15 years I have to give disability retirement due to illness to a person, I am interested in knowing that person's medical history, what pathology he/she had when started to work, so I cannot delete anything, I have to have that information, that remains in the Hospital Information System, a database from which information is extracted.
>
> As regards the update, it is updated to the extent that the worker comes to get his check-ups."

Likewise, in relation to access to said data bases, the interviewees clarify that only the data subject is the one who can have access to his/her medical studies: workers themselves are the ones who request information regarding the data contained and stored in IPS. On the other hand, only physicians have permission to access the health data of workers referred to both the admission medical examination and others that have to do with the proper functioning of an institution such as IPS that provides health services to its insured persons.

In the framework of the protocols that companies must follow to store health data - be it annual medical examinations or the affidavits delivered to IPS – IPS employees affirm that it is not part of their responsibility to fulfill the inspection role over said internal processes of companies:

---

[4] The REI System is a new data processing system via Internet, called Electronic Information Registry through which you can make all movement operations of employees, print the liquidation and then pay cash or directly through the payment system of the adherent banks. More information in: < https://bit.ly/3hpG5WY>.

> "What happens is that you have to differentiate two things. I am a provider of short and long-term health services. The governing body of the Labor Code is the Ministry of Labor and they have a department for this. They have their inspectors who are responsible for this safeguard."

Beyond the list offered by Decree 14.390/92 on the type of medical examination that should be done to workers, the interviewee from IPS states that this is not limiting and that for this reason it is vital that companies consult an occupational physician to study each particular assignment that a worker must do within the framework of his/her duties:

> "This Decree references, but it is not absolute and essential. It is important for companies to hire an occupational physician to define their jobs and inherent hazards."

In relation to the general management of the databases that the IPS has, with respect to the national, internal and international regulations that sustain the management of such, the interviewee states that:

> "In case, by priority, it is the national law. They are data, they are medical reports. So, they have the necessary precautions. We, for example, if a company asks us what illness a certain patient has, only by court order we can inform about it. In fact, IPS cannot give individualized data, medical data, salaries, nothing. Only for statistical purposes some information can be shared with the Ministry of Finance, Civil Registry, etc. and for the purpose of attacking tax evasion and so on. Information can only be given to the data subject, upon request."

The interviewee also clarifies that the data collected by IPS are not used for purposes other than those for which they were collected for, and as regards the question about infrastructure incidents of some kind, they do not remember having suffered any in particular. In any case, he states that they have protection mechanisms and protocols in case there is some type of attack.

Another question for the interviewee was about the location of the IPS servers that store all the information that the institution collects in the framework of its functions. The interviewee pointed out that everything is stored in the country. There is a main server located in the IPS's headquarters and then a mirror in another part of the city (he did not specify where, for security reasons) that protects the data in case of a disaster.

Finally, regarding the obligation of the insured and authorized persons of a patient to register their fingerprints for the collection of medicines granted by

IPS, it is identified that there are not enough regulations that refer to the definition and implication of the biometric data collection by IPS. The only regulations that the interviewees mention for the collection of said data are Resolution no. 003-050/16, which requires the collection of the fingerprints of IPS insured persons.

Regarding the reasons for accessing such biometric database, as well as the permissions and accesses of each employee who can consult it, they state that:

> "All our databases that are here have a confidentiality agreement. I have a username and a password that is confidential to me. If I access and take some information out, it will be registered in the system.
>
> Tomorrow, if there is a problem of data disclosure we can know from what computer and what user it was made. We already had cases in the media with salaries of managers, etc.
>
> Health data, the Hospital System is only available to doctors, and it is also confidential.
>
> The reasons for accessing the database are for access to medication (an ID is presented and then the pharmacy employee can give it to the patient, and that's where the fingerprint is used and it is only for that purpose). All this is stored in the electronic medical database (medical consultations made, how many times medications were collected, how many times was the patient in the emergency room)."

On the risks identified in the biometric databases, he points out that: "[w]e have a specific area of security that identifies the risks and makes the recommendations."

Regarding the enrollment process for the registration of all IPS insured persons to the biometric database, it is still an ongoing process, since although they mention that all retirees have already been registered, the rest of the insured persons are still in the process of registering their fingerprint. The interviewees could not provide an exact number of registered people.

Finally, when asked about potential situations of discretion of IPS employees to sell information to companies and private clinics, they indicate that:

> "Yes, everywhere. As in any organization there are dangers: medical and administrative. There is corruption everywhere, and profit with information. But there is also a strong fight, whoever is caught doing that, is immediately fired."

When the same question is asked but to the private sector and more in the sense of potential situations of discrimination according to the type of degree of health or illness identified to a certain worker, they indicate that:

> "We already have experiences of complaints. This issue of the Admission Medical Examination was very distorted. We do not seek to limit access. But a lot of things were said.
>
> In fact, if we go to the conception itself, the Admission Examination serves as a filter. Because, if for example the three of you apply for a job here and one of you has a disease that is proven that can generate several rest days, obviously I will not hire you. That is why it is called admission.
>
> The issue of HIV that is so taboo, we have complaints from organizations that said that there is discrimination."

Interviews with Employees of the Ministry of Labor

If you use this template, there will be no need to check the page size of your submission. For the purposes of the present research, and in view of the decision to expand the object of the research to also analyze the annual periodic examination required by the Ministry of Labor, an interview was conducted with the Department of Inspection and Supervision of the Ministry of Labor. This seeks to better understand the process of control to companies in the context of the application of this examination.

Specifically, with regard to the type of examinations that workers must take, the employee interviewed makes reference to Decree 14.390/92 as the basic standard, but clarifies that each case is also specific, depending on the hazard:

> "The examinations vary according to each case (Back to Art. 260, 261, and 262 and 263 of Decree 1490 of 1992 establishes what should be taken, as well as the periodicity). They are defined by the Labor Code, and therefore required by the Ministry.
>
> The Ministry demands that those who work in situations of hazards such as, for example, heights, take an examination done by an occupational doctor. The company has the obligation according to each case in particular. And ideally, with an occupational doctor, and not clinical one, but we accept it because there are usually not many."

Also, about risky or unhealthy jobs, refers that the examinations should not be taken every year, but semiannually, to be able to better accompany the evolution and welfare of workers.

On the other hand, and within the framework of whether there is an inspection process to evaluate the safety standards that companies have for the protection of the health data of their workers, he refers that with regard to the obligation of the Ministry of the Labor and its attributions:

> "That is up to the doctor. There are companies that do have and there are others that do not. Those are the ones that are fined, and the fines are very high because they are made according to the number of workers. The Ministry does

> not have a standard of review or care of medical examination data because it does not correspond to it, and it is the full responsibility of the doctor.
>
> Whether or not the medical examination was taken and if the worker is fit or not are the criteria that only the inspector has. These are the main requirements. For more issues, the labor code would have to be modified, and since currently it is not included in it, it is not the inspector's competence, but the doctor's.
>
> There is no contemplated fine or penalty from the Ministry of Labor. It would be necessary to look for a mechanism, perhaps coming from the Ministry of Health. It does not really matter to us."

The interviewee points out that all the protection and access of the data to an inspector are also under the responsibility of the doctor:

> "The company doctor is responsible and can only provide the information to the inspector who requests it. In companies with more than 150 employees, there must be a health department that is responsible for collecting this data. When there are less than 150 employees, there is not a doctor in the company, but there are outsourced doctors who go from time to time. In that case and according to the regulations, it is that doctor who must safeguard the medical personal data of the workers. The main responsibility of the Ministry is to see if the employee is fit to perform the job assigned to him/her. Everything is corroborated on the basis of the National Constitution, the Labor Code and Convention 81, and Act 5115/13, on the creation of the Ministry of Labor and the functioning of the General Department of Inspection."

Likewise, he points out that the Ministry does not collect workers' health data, but is only responsible for monitoring compliance with the regulations in force through its supervisors:

> "The Ministry is not the entity that collects these data. The doctors must store the examinations and the data of the workers while they work there. The Ministry does not collect any type of data in this regard."

Finally, as regards the degree of employers' compliance with the annual periodic examinations, like the Admission Medical Examination, the large companies are the ones that mostly comply with the resolution, as opposed to the medium and small ones, they do not do it in a large number.

Interviews with Private Sector Companies

If you use this template, there will be no need to check the page size of your submission. Both for the Admission Medical Examination and for the annual one, some similar practices are identified and others are different in what refers to

compliance with current regulations for the collection of medical data of workers by companies. Four companies from different sectors were interviewed: academia, media, services sector and pharmaceutical sector.

The four companies are currently complying with the current regulations related to the admission medical examination and also in relation to the annual examination. Some, like that of the "media" sector, already had mechanisms for medical check-ups of new workers and others have just begun to implement these examinations after the IPS regulation.

In the interviews, there are similarities and coincidences identified regarding the process of collecting medical examinations, in the sense that most of the companies outsource the health data collection service:

> "[In the media sector]: The admission examinations are carried out by a hired company, an outsourced service. This company receives the data that are sent by the people.
>
> [In the service sector]: The service is outsourced, we do not do it, we do not collect anything.
>
> [In the pharmaceutical sector]: It takes place during the onboarding process of the worker to the company. It is done by an outsourced service: a private clinic."

On the other hand, the academic sector is in a kind of gray area, in the sense that it is not the company that collects the data, but uses a hospital associated with one of the careers that it offers:

> "We have our own hospital that provides this service to the university community and also for urgencies when IPS cannot help us. The doctors who are working in the hospital send us the reports (professional medical statement)."

A particular situation referred by one of the companies interviewed has to do with the criteria of outsourced clinics when making health examinations to workers, as well as certain irregularities that some doctors perform for profit:

> "The outsourced clinics, contracted by the employer to perform the worker's medical examinations during the onboarding process, usually perform a complete examination of the workers. Their criterion has the purpose of charging more to the company; instead of an examination of 60 thousand guaraníes, they charged 250 thousand guaraníes per person, so it is convenient for them to make a complete examination.
>
> In 2015 we suspended the clinic for requesting health information beyond what was requested by us. I think this was not to sell more information to others necessarily, but to charge us more."

Another problem that we found is that doctors usually give you the medical certificate without performing the examinations, it is a little more expensive but they certify the company for faster registration to IPS. We do not accept it, but it is something that exists in the market.

On the other hand, it is noteworthy that in all the cases referred to the access of health data collected - whether affidavits or the medical examinations themselves - only human resources personnel have access to such files. In all cases, workers also have full access to their data, upon request:

> "[In the services sector]: Only the Human Resources personnel who are two people. And we give a copy of those results to the workers, in fact they ask you because they never take any type of check-ups and it is the only time in their life that they get a complete medical check-up.
>
> [In the media sector]: Only the Human Resources department and the worker. A copy can be given to the worker upon request. In this department there are only 4 people, and all of them handle this information.
>
> [In the academia sector]: we do not see the results of the examinations because it is a matter of patient-doctor. The university does not receive any electrocardiogram, tomography, clinical analysis or doctor's opinion. There is only one sheet that technically the Personnel Department usually gives the professor and that is the sheet that the doctor signs saying the person is fit or not for the particular assignment.
>
> [In the pharmaceutical sector]: The area of human resources of the company has access to it. The original results are given to the workers."

On the other hand, for all cases, companies receive and handle affidavits and medical results in printed format. Only the academia sector claims not to store medical results that are delivered only to workers. In the case of the other 3 companies:

> "[In the services sector]: Only printed, nothing digital. They send you the pre-established form with the patient's questions and answers plus the examinations that were performed to them and they send you everything on paper, and we file it, keep it in a folder that is specific to the medical examinations and is managed by a human resources person and there is no other person with access to that, because it is under lock and key.
>
> [In the media sector]: Printed, they keep it in the file of the people in the Human Resources department.
>
> [In the pharmaceutical sector]: We only have documents in printed format. We only have a medical certificate. The doctor who makes the certificate has the data of the worker's examinations, and all that is stored in the file of each worker under lock and key.
>
> The original results are given to the workers, we keep a copy, and then we see if it is necessary to follow up on any disease that needs to be treated."

All the companies interviewed affirm that all workers have access to their files and medical records upon request. On the other hand, another coincidence found in 2 of the companies interviewed has to do with the fact that they do not destroy the health data they collect about their workers:

> "[In the media sector]: We do not delete the databases.
>
> [In academia sector]: We really leave that in the file, which was the indication given to us. We cannot suddenly throw it away because anything can happen if you do it, unless you incinerate it but then that is an environmental matter and is another problem. So, it is kept in the file."

Of the other two companies interviewed one adduces reasons that have to do with the fact that they have been applying the law for a short time. According to the interviewee, documentation has not yet been destroyed due to the Accounting Act that requires the storage of legal and fiscal documents for 5 years, and they use this same criterion for personal data. The other company uses the same criteria also when destroying documentation:

> "[In the services sector]: No, because the law requires you to keep all types of documents for 5 years. After 5 years, we will for sure burn and throw everything away. Since it is something new, we do not have a 15-year database of these issues. But we will destroy everything after 5 years as we do it with other documents.
>
> [In the pharmaceutical sector]: Yes, every 5 years. We do not have any written protocol, it's just verbal."

Also, in the cases of the sectors of services, pharmacy and academia, they are dedicated to studying the particular role of each assignment, to determine what type of examinations should be applied to an incoming worker. In the case of the media sector, they are governed only by Decree no. 14390/92 on Hygiene and Health:

> "We are guided by what is required by the Act established by the Ministry according to its regulations."

Finally, on the consultation of the possibility of discretion of IPS employees for the sale of health data to clinical and pharmaceutical companies, none of the interviewees make assertions about it, varying the arguments of why:

> "[In the service sector]: I do not know, neither is it ... when you send the data, they ask you for very basic things, they do not ask for diseases: they ask

> if the person is fit or not, if the person has some health problems, more or less, it is just a matter of yes or no.
>
> They ask for the doctor's name and registration. It's only for IPS to make sure that the company did the admission medical examination and shield themselves from the favor insurance. Really, with the information asked for in the website, there is not much they can do.
>
> [In the media sector]: I do not think so, IPS carries out this for the insurance of favor, and I do not believe that there can be a particular interest of the people of IPS given the fact that the admission examinations are requirements for all the companies.
>
> [In the academia sector]: The insurance of favor is a problem and this whole issue of the admission exam can palliate it. However, there needs to be a special care with the data management information that is essential, because they are rights of third parties.
>
> [In the pharmaceutical sector]: No, IPS takes too long for basic blood tests, therefore it is done with another company for registration to IPS."

CONCLUSIONS AND RECOMMENDATIONS

The challenges mentioned clearly illustrate how the field of technology, health, rights of privacy and confidentiality of personal data, become a very complex field, both from the legal point of view and the integrity and dignity of the people. This calls for more attention from the Paraguayan State, as well as it should be a focus of interest of the academy, in the field of health.

The trivialization of the collection and exchange of sensitive health data and fingerprints require greater attention by the competent authorities to control the amount of health data that are currently being collected by public and private sectors. For this, the development of technologies that allow the implementation of standards for the protection of privacy and confidentiality with respect to personal health and biometric data, in order to avoid carelessness by health administrators, will be indispensable.

On the Admission Examination and the Annual Examination

When dealing with medical examinations required by IPS and the Ministry of Labor, it is necessary to recognize that **guarantees are needed to ensure that the mechanisms are adequate.** That is, that each mechanism is specifically applied to the working conditions that the person will be assigned to and avoid putting their environment at risk. It seeks to generate a healthier work ecosystem where there is protection for the worker, coworkers and the employer itself.

The challenges that technologies propose for the right to privacy and confidentiality are many. Society has evolved in ways that seem to contradict the

importance of these rights in the past. However, the evidence that emerges from this research makes it possible to ensure that the protection of rights with respect to personal health data remains a priority for patients and physicians.

Beyond the annual medical examination that has been obligatory for years, **most of the interviewees mention that the obligation of these examinations is very recent.** The admission medical examination is of recent implementation, which is why it is in a phase of application on the part of the employers who are registered in IPS. Because of this, successive resolutions of the Board of Directors of IPS have postponed the application of fines for those who do not comply with the regulations in this regard. **However, it is assumed that progressively more employers will have to comply with said regulations.**

On the side of those companies that are currently in compliance with these regulations, the findings show that the norm is **the discretion or intuition of the employers and managers in charge of the management of human resources.** That is, they do not have practices or standards related to the management of workers' health data.

With regard to the collection and systematization of health data of workers by third parties (outsourcing), common practices were found. However, one of the people interviewed pointed out that it is common to request more examinations than necessary by some clinics. **With this, they charge more money and it becomes worrisome, as well as a violation of workers' rights, leaving them in a situation of potential vulnerability.**

The fact that all the companies assure that access to health files is the exclusive right of each worker, that is, the data subject, stands out as positive. In the case of companies that keep medical examinations, the same thing happens.

Of the companies interviewed, there are some with greater care when analyzing which health data, they need to keep, avoiding the unnecessary storage of data. Only one of the companies interviewed said that they only keep the affidavit form required by IPS, as well as the fitness certificate of the workers. The rest of the companies interviewed keep even the results of medical examinations, and although they deliver the original document to the workers, they keep a copy for the company's archive, without there being any real justification for it. **In all cases, the companies keep this data in printed form and under lock and key.**

Another worrisome fact related to the previous point is that both the Ministry of Labor and IPS do not actively assume the role of control over the way in which the documentation required by their own regulations and provisions is protected. No convincing criterion or argument is identified that exempts the responsibility of these institutions in relation to their role in controlling that companies manage the health files of their workers in a proper

manner. **Based on the interviews conducted, a worrying gap is identified when a public entity or body guarantees that the security measures of the companies' health files are stored according to the appropriate standards.**

Another worrisome identified trend is the lack of a general protocol that contemplates the destruction of sensitive health data - and data in general - of workers, once the purpose for which they were collected was accomplished. The majority of the companies and public entities interviewed keep the databases for an indeterminate period of time, or for longer than necessary. It is a reality that must be corrected with regulations in accordance with the highest standards of personal data protection.

On the other hand, both IPS and the Ministry of Labor pointed out that the majority of the large companies comply with these regulations, while small and medium-sized companies are in a high degree of non-compliance. It is necessary to study this phenomenon in greater depth in order to understand why the legal requirements in this sector are not being met and therefore the maximum welfare and protection for workers is not being ensured.

Regarding the definition of the **type of medical examinations** that can and should be performed to workers by companies, some define them with the advice of doctors, but there could be potential situations in which companies ask for more medical examinations than necessary, which can lead to situations of discrimination. There have been complaints about requesting HIV studies during the onboarding process, which is in clear violation of current legislation. Although IPS has taken measures, clarifying that it is not necessary to request this kind of information, a commitment must be identified by the authorities so that these violations of rights do not happen again.

Regarding the collection of health data of the insured person in IPS, the principles that govern the collection of personal data in general are applicable. In this case, the standards expressly established for the treatment of sensitive data must be taken into account.

The principle of **data quality** must be respected, that is to say that the data collected must be adequate, relevant and not excessive in relation to the scope and purpose for which they were collected. Also, its collection cannot be done by unfair, fraudulent means or in a manner contrary to the legal provisions, nor can the data be used for purposes that are different or incompatible with those that led to its collection.

Thus, and with particular reference to the admission and annual medical examination, **it is necessary to reiterate the urgent need for an comprehensive act for the protection of personal data** that has the attributions and competent authority necessary to balance and clarify the practices and standards related to the collection, storage and communication of personal health data of workers.

This applies not only to companies and employers, but also to public entities that require the collection and store this type of data.

On the Biometric Data Stored in IPS

It is necessary that there is greater speed in the adaptation of certain practices, since the continuous transformations in society constantly bring new facts that impact on privacy and confidentiality, such as patients' rights. This applies both to medical research or medical care environments, and to the storage of fingerprints of people insured in IPS. More and more people adhere to the free information and are ignorant or reluctant to the principles of data protection, until they suffer considerable consequences.

The collection of biometric data (fingerprints) was implemented without an adequate legal framework. Without one, the treatment of such data cannot be guaranteed in a proper manner by the State or the private sector. In case of abuses or filtering of biometric data, the State does not have a competent authority to ensure the protection thereof.

The biometric data are sensitive data, which requires greater safeguard mechanisms that this draft law does not contemplate. In the resolution of the IPS Administrative Council, the challenges to guarantee the care of the data in the face of discriminatory practices, biases in the development and implementation of the biometric data collection software are not taken into account. It is also important to clarify that with mere consent, it is not a sufficient legal argument to deal with biometric data.

The technology and mechanisms that will be used for the collection, analysis and storage of the biometric data, as well as the scope of this policy, are unknown. Who will have access to the biometric data? Will they be shared and transferred between different public or private organizations? Which State institutions will access these data and can it be guaranteed that the request for biometric data is made through a prior judicial order in cases of criminal investigations? Are safeguards provided to prevent manipulation and adulteration of stored fingerprint copies? Will there be sanctions in case of abuses by those responsible for the databases or the authorities? These are just some questions that arise in the analysis.

The collection of biometric data is disproportionate. Fingerprints can be a more control mechanism that could aggravate surveillance practices and harassment of minorities, ethnic groups, immigrants, and so on. The failure of the State to take care of citizens' private information makes these records even more problematic and with a high risk of being filtered.

There is no impact evaluation of the use of biometric data systems. A previous impact analysis was not conducted to evaluate the importance of the

implementation of a biometric data collection system. Any interference by the State must be based on solid foundations, based on data and serious and independent diagnoses, in order to meet the conditions of necessity and proportionality required for the legitimacy of any measure that seeks to limit fundamental rights.

Finally, it should be emphasized that the only defense against the risks of abuse by public authorities and private corporations is to strengthen the regulations around privacy and confidentiality as well as data protection rights in health care.

In the research carried out on databases in the public sector (ACUÑA; ALONZO; SEQUERA, 2017), published together with Privacy International, the systematized problems and recommendations highlight **the strong necessity of an integral personal data protection law in Paraguay.**

In the current legislation, health data are still considered particularly sensitive and vulnerable in relation to fundamental rights or privacy, but they deserve specific protection. The future regulations must take into account not only the defense based on human rights, but the creation and defense of more inclusive and reliable economic models in the online environment.

REFERENCES

ABC COLOR. ***Fingerprints Are Taken to Collect Medications,*** September 3, 2016. Retrived from: <https://bit.ly/3bZyw8g>.

———. ***Tons of Irregularities,*** April 23, 2019. Retrived from: < https://bit.ly/2RpYJmS>.

ACUÑA, J; FULCHI, L. A; SEQUERA, M. ***La Protección de Datos Personales en Bases de Datos Públicas en Paraguay.*** Un Estudio Exploratorio. TEDIC, 2017. Retrived from: < https://bit.ly/2Zz2qeA>.

ASOCIACIÓN POR LOS DERECHOS CIVILES. ***The Identity We Can't Change***. How Biometrics Undermine our Humanrights, 2017. Retrived from: <https://bit.ly/3hsSBoN>.

EUROPEAN UNION. ***Regulation (EU) 2016/679 of the European Parliament and of the Council,*** on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Retrived from: <https://bit.ly/2ZCsJAC>.

FARIA, P. L. de; CORDEIRO, J. V. Health Data Privacy and Confidentiality Rights: Crisis or Redemption? ***Revista Portuguesa de Saúde Pública***, vol. 32, n.2, 2014, p. 123-33.

FERREYRA, E. ***ADC Biometrics and Protection of Personal Data.*** Buenos Aires: Asociación por los Derechos Civiles (ADC) Digital, 2017.

GAETE, R. ***Financiamiento de la Cobertura Universal de Salud en el Paraguay***. Paraguay Debate, 2017. Retrived from: <https://bit.ly/3iwpeDh>.

INTERNATIONAL LABOR ORGANIZATION. ***About ILO.*** Retrived from: < https://bit.ly/3ml5sgn>.

_____. ***Protection of Workers' Personal Data***. An ILO Code Of Practice. Geneva, International Labour Office, 1997. Retrived from: <https://bit.ly/2RtX9Au>.

_____. ***C111 - Convenio sobre la Discriminación (Empleo y Ocupación)***, 1958. Retrived from: < https://bit.ly/2ZGd43o>.

_____. ***C161 - Convenio sobre los Servicios de Salud en el Trabajo***, 1985. Retrived from: <https://bit.ly/3kfjJcw>.

_____. ***R171 - Recomendación sobre los Servicios de Salud en el Trabajo***, 1985. Retrived from: <https://bit.ly/35Bk9pz>.

_____. ***Hechos Concretos sobre la Seguridad Social***, 2018. Retrived from: <https://bit.ly/3hEILQR>.

LUNA, J. R; SEQUERA, M. ***State Communications Surveillance and the Protection of Fundamental Rights in Paraguay.*** TEDIC and Electronic Frontier Foundation, 2016. Retrived from: <https://bit.ly/2DZfRNg>.

ORGANIZACIÓN MUNDIAL DE LA SALUD. ***Indicadores Básicos de Salud: Paraguay 2017.*** Retrived from: <https://bit.ly/3kfnDCc>.

PARAGUAY. Boletín Informativo. ***Noticias del Instituto de Previsión Social***, Año 8/2018-Nº 104. Retrived from: <https://bit.ly/33r2TRm>.

_____. Congreso Nacional. ***Ley no. 1682/2001,*** reglamenta la información de carácter privado. Retrived from: <https://bit.ly/2RozIJ3>.

_____. Congreso Nacional. ***Ley no. 4933/2013***, que autoriza la incorporación voluntaria de trabajadores independientes, empleadores, amas de ca y trabajadores domésticos al seguro social – Fondo de Jubilaciones y Pensiones del Instituto de Previsión Social. Retrived from: <https://bit.ly/3khz4cz>.

_____. Constituent Assembly, 1992. ***National Constitution of the Republic of Paraguay.*** Retrived from: < https://bit.ly/3hxRZOH >.

_____. Instituto de Previsión Social. ***Misión, Visión y Objetivos Estratégicos***. Primera Parte del Plan Estratégico Institucional (PEI) 2020-2024. Retrived from: <https://bit.ly/3kfoB1i>.

_____. Instituto de Previsión Social. ***Aspectos generales del Seguro Social y del IPS***, 2017. Retrived from: <https://bit.ly/3irSISG>.

_____. Ministerio de Justicia y Trabajo. ***Resolución no. 730/2009***, por la cual se releva la fe de erratas del Reglamento General Técnico de Seguridad, Higiene y Medicina en el Trabajo, aprobado por el Decreto no. 14390/92, en cual consta que el examen médico admissional, Test de Elisa, es obligatorio. Así mismo se reglamentan disposiciones referentes al Test de Elisa en el lugar de trabajo, observando las recomendaciones prácticas de la OIT y la Declaración de Compromiso UNGASS 2001. Retrived from: < https://bit.ly/2DZY8VZ>.

_____. ***Plan Nacional de Ciberseguridad***, 2016. Retrived from: <https://bit.ly/3ive9m0>.

_____. Presidencia de la República. ***Decreto no. 7052/2017***, por el cual se aprueba el Plan Nacional de Ciberseguridad y se integra la Comisión Nacional de Ciberseguridad. Retrived from: <https://bit.ly/3bZGCOc>.

PRIVACY INTERNACIONAL. ***Biometrics: Friend or Foe of Privacy?*** Briefing, 2017. Retrived from: <https://bit.ly/3bYNV8K>.

SERAFINI, V. ***Guidelines for the Construction of the Social Protection Policy.*** Paraguay Debate, 2017. Retrived from: <https://bit.ly/32xJU8t>.

UNITED NATIONS. UN Rights Chief Urges Protection for Individuals Revealing Human Rights Violations. ***UN News***, 2013. Retrived from: <https://bit.ly/33wUprA>.

_____. ***Declaración Universal de Derechos Humanos***, 1948. Retrived from: <https://bit.ly/2ZBL2WL>.

_____. Human Rights Council. ***Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expresión, Frank La Rue.*** A/HRC/23/40, 2013. Retrived from: <https://bit.ly/3c0CYnk>. _____.