PRIVACY AND CONFIDENTIALITY – WHO HAS ACCESS TO THE DATA IN CLINICAL CARE PERSPECTIVE. HOW TO INCORPORATE BIG DATA IN A LEARNING HEALTHCARE SYSTEMS SETTING?

EULAC-PerMed

MARÍA ISABEL CORNEJO PLAZA
Lawyer, LL.M, Phd ©
isabelcornejo@derechocivil.cl

DISCLOSURES

No disclosures.

CONTENTS

- Introduction.
- Legal framework for the protection of privacy and confidentiality in health care in Chile.
- Legal framework for the protection of privacy and confidentiality in health in comparative law.
- Who has access to the data in clinical care perspective?
- How to incorporate big data in a learning Healthcare system setting?
- Conclusions

LEGAL FRAMEWORK FOR THE PROTECTION OF PRIVACY AND CONFIDENTIALITY IN HEALTH CARE IN CHILE.

Privacy and confidentiality are two primary values that safeguard the dignity of people and patients. Big data in health understood as a large volume of data with sensitive content for the patient can become a tool that, through good regulation, can help move from curative to preventive medicine and be used for the benefit of the patient.

However, misuse can not only violate the law, but can have unusual biopolitical consequences.

LEGAL FRAMEWORK OF THE RIGHTS AND DUTIES OF PATIENTS

- Political Constitution of the Republic.
- International Treaties and Bioethical declarations as soft law.
- Health Code.
- Law 20.584 (Patien´s bill of rights).
- Law 20.120 (Scientific research on the human being, its genome, and prohibits human cloning).
- Law 19.628 (For the protection of private life)

LEGAL FRAMEWORK FOR THE PROTECTION OF PRIVACY AND CONFIDENTIALITY IN HEALTH CARE IN CHILE

Law 19.628 has been in existence for 21 years, and is an obsolete law, so it is said that its scope is very limited given the complexities big data. In this sense, there has been a bill for more than 4 years that attempts to modernize the data protection law.

LEGAL FRAMEWORK FOR THE PROTECTION OF PRIVACY AND CONFIDENTIALITY IN HEALTH IN COMPARATIVE LAW

The legal framework for data processing presupposes that the data must be collected for specific, explicit and legitimate purposes, principles included in the GDPR which comes into force in May 2018. However, by definition, research backed by genomic medicine no 'has no specific purpose and the consent given by the patient to the examination of his genetic characteristics and other medical data in the cohort cannot be clarified as to the precise purpose pursued by the research (s) of which he will be subject.

LEGAL FRAMEWORK FOR THE PROTECTION OF PRIVACY AND CONFIDENTIALITY IN HEALTH IN COMPARATIVE LAW

However, this inclusion is not neutral, in particular with regard to the risks incurred by the patient for his private life. We know that cyber-attacks, including on national health systems, are daily. We also know that the re-identification of a person becomes possible from cross sequences with "minimal" data contained in open access databases. This once again questions the validity of consent. Therefore, the anonymization of data cannot be seriously guaranteed and the question arises, on the one hand, of the responsibility of hosts and data processors; on the other hand, the insurability of this risk for the hosts and, where applicable, for the patient.

“PROTECTED HEALTH INFORMATION”

- “Protected health information” includes any identifiable health information relating to the health of an individual, the care provided or payment for care
- PHI includes information in any form or medium: electronic, paper, oral…

DE-IDENTIFICTION

- De-identification requires that identifiers of an individual or of relatives, employers or household members are removed, including:
  - Demographic information
  - Locating information
  - Elements of dates (birth date, admission date, discharge, date of death, etc.)
- If health information de-identified, information can be used without an authorization from the patient for research or other uses.

LIMITED DATA SETS

- Permits use of limited data sets for research, public health and health care operations purposes without authorization.
- Requires removal of directly identifiable information (name, address, medical record number, etc.
- Requires data use agreement between Covered Entity and user of information
- Recipient must agree to limit the use of the data set for the purposes for which it was given, and to ensure the security of the data, as well as not to identify the information or use it to contact any individual.

PREPARATORY TO RESEARCH

- No authorization or waiver required if:
  - Use/disclosure sought only to prepare a research protocol or for similar purposes preparatory to research.
  - Researcher will not remove PHI from the Covered Entity’s premises.
  - PHI for which use or access is sought is necessary for the research purpose.
  - Only de-identified PHI is recorded by the researchers
- Entity must obtain assurance from researcher that the above requirements are met.

WAIVER REQUIREMENTS

Research could not be conducted without the waiver.

Research could not be conducted without access to and use of the PHI (Protected Health Information).

Disclosure involves no more than minimal *privacy risk* to the individuals.

-Adequate plan to protect the PHI

-Plan to destroy the identifiers

-Adequate written assurance from the investigator that the PHI would not be reused or disclosed.

WHO HAS ACCESS TO THE DATA IN CLINICAL CARE PERSPECTIVE?

- Patients must have access to their data. Also have the right to not know.
- The doctor and the patient's treating team and health insurance companies.
- On the other hand, European legislation on the protection of personal data imposes the principles of transparency and loyalty in the treatment of personal data and medical software.

WHO HAS ACCESS TO THE DATA IN CLINICAL CARE PERSPECTIVE?

These terms still need to be defined. **Transparency** is usually understood in a narrow way, as the imposition of revealing the algorithmic code used by the software.

However, such transparency is contrary to the industrial secret. **Loyalty** refers to the idea that the software must correctly perform the service expected by the buyer or user without betraying them. Loyalty is, therefore, part of respecting ethical, legal and moral standards. However, its field of application is ambigous.

WHO HAS ACCESS TO THE DATA IN CLINICAL CARE PERSPECTIVE?

- First, the right to personal data, which can be found within the European Data Protection Regulation 2016, offers only limited information to patients whose data is subject to algorithmic processing.
- Certainly, there are provisions related to the patient's right to obtain an explanation of how an algorithm works:
- Article 13 of the regulation requires, therefore, that the data controller informs the person whose data will be processed, when they are collected:

WHO HAS ACCESS TO THE DATA IN CLINICAL CARE PERSPECTIVE?

- Or the existence of automated decision-making (article 13 (2) (f)) or and in this case, useful information about:
- the underlying logic, the importance and expected consequences of this processing for the data subject.
- Article 15 requires, similarly to Article 13, that the person, whose data has been collected, can be obtained from the processing of said information.

WHO HAS ACCESS TO THE DATA IN CLINICAL CARE PERSPECTIVE?

Article 22, indicates that the person affected by data processing can oppose a decision regarding exclusive automation in two situations:

(I) when the processing produces legal effects on the person or (II) when it similarly affects [the legal effects] significantly. This prohibition in principle has exceptions in three cases, two of which are of special interest to us:

WHO HAS ACCESS TO THE DATA IN CLINICAL CARE PERSPECTIVE?

Firstly when this automated processing necessary for the conclusion or execution of a contract is carried out (article 13 (2) (a)) or secondly when the interested party has given their consent (article 13 (2) (c))

In these cases, the regulation establishes that the data controller must "implement the appropriate measures to safeguard the rights and freedoms and the legitimate interests of the interested party."

WHO HAS ACCESS TO THE DATA IN CLINICAL CARE PERSPECTIVE?

These appropriate measures can be understood in the context of a right of the person to obtain an explanation about the way in which the data processing works and that motivated the adoption of the decision that concerns him.

HOW TO INCORPORATE BIG DATA IN A LEARNING HEALTHCARE SYSTEM SETTING?

Big data must be safe, intelligible for patient and physician. A proactive interpretation of the personal data law can provide a basis for the rights of patients in this area as well as for physicians. It is also possible to think about the creation of a general contractual obligation of reinforced information at the expense of the manufacturers of the software used for the benefit of any user: consumer or professional, and this in view of the risks posed by the use of these software. This is the first step to implement a system for learning these technologies by doctors and patients.

Thank for your attention!

isabelcornejo@derechocivil.cl