RESEARCH DATA ALLIANCE

Health Data Interest Group @P10

Health data mapping and diverging trends in health data protection

21 September 2017, 9:00-10:30

Diverging data protection regulations and security standards referring to health data

Ludovica Durst

research data sharing without barriers

rd-alliance.org

Background: Data protection has become a global issue

- Almost all countries have developed legislations with regards to privacy and data protection or participate to some kind of international/regional cooperation establishing a legal framework
- Many of them also have dedicated legislation or special rules and provisions governing health data

(reference: Data Protection & Privacy International Series, 2016)

Background: Data protection has become a global issue

- Some examples of international legal framework on regional basis:
  - 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data
  - 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe (also some non-European countries are recently acceding)
  - 2004 APEC (Asia-Pacific Economic Cooperation) Privacy Framework (non-binding 9 principles minimum standard, based on the OECD Guidelines)
  - Global Privacy Enforcement Network (GPEN) for cooperation among enforcement authorities

Diverging trends in privacy and data protection (health data)

- US model: sectorial self-regulatory approach

- EU-style: comprehensive data protection laws

Diverging trends in privacy and data protection – US model

- US model: sectorial self-regulatory approach
  - **HIPAA** (Health Insurance Portability and Accessibility Act), 1995 is the federal law that regulates health privacy, enforced by the US Department of Health and Human Services (HHS)
  - HIPAA was strenghtened by the Health Information Technology for Economic and Clinical Act (**HITECH Act**) 2009
  - HIPAA both requires to accomplish **compliance** and **security**, including:
    - The Privacy Rule
    - The Security Rule (basic security standards for storage and transfer of data)
    - The HIPAA Breach Notification Rule (circumstances under which covered entities must inform consumers of a data breach)

Diverging trends in privacy and data protection – US model

- US model: sectorial self-regulatory approach
  - Title II in particular provides for national standards to protect the privacy and security of **personally identifiable health information (PHI)**,
    - limiting the circumstances in which PHI can be disclosed by certain entities (covered entities and business associates),
    - or when the data subject has given consent in writing
  - PHI can be de-identified by a covered entity or a business associate by
    - determining that the risk of identifying an individual is very small;
    - by removing a list of 18 specified identifiers
  - HIPAA Privacy Rule will not supersede a contrary provision of **State law** if the provision is more protective of privacy than the HIPAA Privacy Rule

Diverging trends in privacy and data protection –EU approach

- EU-style: comprehensive data protection laws
  - **GDPR** (General Data Protection Regulation) repealing EU Directive 95/46/EC of 1995, entered into force 25 May 2016 and to be applied from 25 May 2018
  - **Health data** qualifies as a special category of personal data (sensitive data) subject to stricter processing conditions
  - There is no sector-specific EU framework for data protection in the **health sector**
  - the GDPR provides for a specific framework for processing of personal data for **scientific research purposes**, which shall be subject to appropriate safeguards aimed at ensuring that technical and organisational measures are in place, such as pseudonymisation, in light of the principle of data minimisation.
  - EU **member States** may introduce further conditions, including limitations, for the processing of specific categories of data, such as health data

Categories of data under the scope of EU data protection law

Personal data

Personal data is defined as any information relating to an identified or identifiable natural person. An identifiable person is one who can be identified both directly and indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

(Recall Health Data IG session at P9 Barcelona and the presentation by Rocco Panetta, Secretary General of Italian Compliance Forum, on *How to define anonymization and pseudonymisation of Health Data*)

Under the scope of EU data protection law

Anonymous/anonymized data

Anonymous data is any information from which the person to whom the data relates cannot be identified, whether by the company processing the data or by any other person/legal entity. The threshold for anonymization under EU data protection law is very high and absolute, meaning that the company's intent is not relevant. Data can only be considered anonymous if re-identification is impossible for any party and by all means likely reasonably to be used for this purpose.

Anonymized data is no longer considered personal data and is thus outside the scope of EU data protection law.

Under the scope of EU data protection law

Pseudonymous data

Pseudonymisation is a form of de-identification, in which information remains personal data. The EU General Data Protection Regulation ("GDPR") defines pseudonymisation as "*the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information*." The key legal distinction between anonymised and pseudonymised data is its categorization as personal data.

Pseudonymous data still allows some form of re-identification (even indirect and remote) and so **falls within the scope of application of EU data protection law.**

As pseudonymisation is considered to ensure privacy-by-design and to be a strong security measure, some exemptions and/or simplifications apply to pseudonymous/pseudonymised data.

Categories of data under the scope of EU data protection law

- Some exemptions for research purposes:

Sensitive data: prohibition of processing genetic and health data, or data concerning sex life, shall not apply when such processing is necessary for **scientific purpose** and appropriate security measures are in place.

Compatible purpose: personal data must be collected for specified, explicit and legitimate purposes and not be further processed in a manner that is incompatible with those purposes.
Nonetheless, further processing for **scientific research** must not be considered to be incompatible with the initial purposes, where adequate security measures are in place for data subjects’ rights.

Right to erasure: “right to be forgotten” shall not apply to the extent that the relevant processing is necessary for **scientific research**, in so far as said right is likely to render impossible or seriously impair the achievement of such purpose.

Influence of the models

- Recently, national regulations appear to be influenced more by the EU data protection approach (Australia, New Zealand, Hong Kong, Japan)
- This influence is also evident in Latin-American countries
  - “habeas data rights” were introduced in many constitutions, starting from Brasil in 1988
- Moreover, the European Commission can assess the “adequacy” of the third country (equivalent level of protection) to transfer personal data to a third Country outside the EU
  - Australia, Canada, New Zealand, Switzerland are on the “white list”

A relevant theme

- Complex but converging global norms seem to be growingly lead by the EU model and approach: can it be said the EU data protection framework is increasingly becoming the global norm (“gold standard of data protection”)?
- Let’s think about it within our HDIG activities!

Some actions towards Berlin P11

- To have a draft Report on the impact of the GDPR on Health Data and related issues, highlighting different data protection standards worldwide (US/North America, Australia/Pacific area, etc.)
- To discuss whether establishing a dedicated working group on this purpose would make sense

How to get prepared for P11 Berlin (21-23 March 2018)

- Around 4 TCs (November-February) on relevant issues: which ones?
  - access/sharing/portability?
  - anonymization/pseudonymization?
  - consent?
  - does the GDPR take into account how new technolgies like blockchain can be applied to health?
  - ...?
- Who would like to be involved?

Thank you!

- l.durst@lynkeus.com