FUTURE OF PRIVACY FORUM

Draft Presentation

Draft Regulation – Review

Patient Rights Regulations (Health Data Research use), 2019

Limor Shmerling Magazanik, Managing Director

limor@techpolicy.org.il

Noam Rosen, Adv , Policy Counsel

nrosen@techpolicy.org.il

ISRAEL
TECH POLICY INSTITUTE

Agenda

- Regulations objective
- Background
- Resolution 3079
- Legal basis
- Regulation principals
- Applicability
- Definitions
- General use principals
- Right to Object
- Health organization obligations
- Approval mechanism
- Anonymization
- Researcher obligation
- Data sharing principals
- Process summary

Regulations objectives

To balance the desire to encourage and promote research collaboration in health data with the requirement to **protect the privacy and confidentiality of medical data**, in order to

1. Improve the medical care quality in Israel, and
2. Promote medical research and human knowledge in health.

Background

- In the 1980s and 1990s, Israel's public health care was a global pioneer in implementing information systems.
- The use of those systems created extraordinary capabilities and opportunities on a global scale to improve patient care and promote innovation.
- In March 2018, the Israeli Government passed Resolution 3079

"A national program for the promotion of Digital Health as a means of improving health as a growth engine to remove barriers and respond to these challenges in an orderly and comprehensive manner "

Resolution 3079

Legislation or delegated legislation drafting principles

1. Proper use purposes;
2. Respect for the right to privacy and medical confidentiality, including the right to a person's autonomy over his data uses;
3. Transparency and ongoing public disclosure concerning secondary uses;
4. Prohibition to discriminate and stigmatize a community or group;
5. Providing access to health data for social solidarity.

Legal basis

The Patient Rights Act, 5756-1996

Section 20 - A medical institution may share health data subject to a patient consent or for a research purpose provided that it's not disclosing patient identifying details. The Health Minister will determine the conditions.

People's Health Regulations (Medical Experiments in Humans), 5741-1980

Every precaution must be taken to preserve the privacy of the person used for the research, and to minimize the harm to the patient in its physical and mental integrity and personality.

Privacy Protection Law, 5741-1981

A person's health condition falls within the definitions of both 'data' and 'sensitive data'. Medical information constitutes a person's 'private affairs'. Infringement of the obligation of secrecy by data use or transfer would constitute an infringement of privacy unless the person gave an informed consent (Inc. implied)

Today, secondary health data use for research purposes is done according to historical arrangements established by virtue of the PPL and Medical Experiments in Humans regulation.

State Health Insurance Law, 5754-1994

This law regulates the activities of the HMOs. It includes their relationship with the insured patient in the treatment of data collected about the patient. Section 60 - The Health Minister may issue regulations on any matter relating to this law implementation .

Regulation Principles

- Propose an approval mechanism for health data secondary use, which includes examination by a professional and internal ethical committee and setting standards for approvals.
- A privacy protection model based on three complementary safeguards (allows to adjust the safeguards taken to the level of risk of harm to patient privacy)

1) **Normative** - provisions and duties applied to health data receivers and data subjects choice and consent requirements;
2) **Technological** - privacy and security measures, de-identification;
3) **Procedural** - mechanisms for examination and approvals.

Applicability

- The regulations apply to health organizations, most of which are subject to the regulatory authority of the Ministry of Health.
    - A health maintenance organization (HMO);
    - Hospitals of a specific size;
    - Evacuation and rescue organizations;
    - The IDF and the Prison Service; and
    - The Ministry of Health;
    - Other health-related org subject to the MOH General Director decision.

Definitions

Health Data	means broad information that directly or indirectly relates to a person's overall health or physical or mental health and includes information on behavior that may affect health status such as exercise, smoking, nutrition, and habits.
Research Use	means the use of health information for research purposes, including providing access for health information or its delivery for such a purpose, except data provided for medical care or service to the patient who is the data subject, or if the patient gave his consent to the secondary use.
Identifying item	includes unique characteristics of the person that can unequivocally attest to their identity, including first and last name, ID, driver's license number, facial image, contact details, and payment method., ID number given by a health organization, except for a number assigned in the anonymization process.
Identified data	means health data about a particular person, contains an Identifying item.
Identifiable data	Health data about a particular person, which does not include Identifying items, but can, with reasonable effort, identify the data subject, including through the use of other data sources.
Anonymized data	Health data that has undergone a process according to Regulation 13 and approved by the committee for particular research use, and under the circumstances of this research use, it is not possible, with reasonable effort, to re-identify the data subject.

General use principles

1) Prohibits anyone from researching health data unless obtaining the internal committee's permission.

2) Only be approved for a specific purpose which is

   - proper;
   - related to health;
   - in the benefit of individual or public health, or
   - can contribute to improving the quality of health care, medical or medical research, and the human knowledge promotion in the health sector; and
   - **The internal committee will approve it only if the expected research benefits outweigh the risk that this anonymized data will infringe the privacy of the patients.**

3) Only with anonymized data, and the minimal extent of data to achieve the desired research purpose.

4) When targeting a specific subordinate population within the framework of which it has given medical treatment, it will only be approved if this same group is expected to benefit from such research.

Right to object

- Data subject has a right to object (opt-out) at any time to secondary research use of health data concerning him or her.
- Data subject has a right to return from his objection at any time.
- Exercise of the right will be done through a national mechanism established by the Health Ministry and will be valid to all health organizations to which the regulations apply.

Health organization obligations

- Comply at least with the InfoSec regulations requirements for databases subject to the high level of data security.
- Share data only with those that are knowledgeable and familiar with the field of health data research
- Request the researcher to sign an undertaking (agreement) and in particular
  - Confidentiality clause; and
  - Commitment to refrain from re-identifying the data.
- Publicly disclose its health data secondary use policy, including
  - Privacy Policy;
  - The threshold requirements for health data sharing;
  - Composition of the organization internal Committee;
  - Details of procedures to request health data access;
  - Information on the approval of an application, details of the research, the types of data used, and the principal researcher.
- Appoint an internal organizational commissioner to handle complaints

Approval mechanism (1/2)

- Health organization shall establish an internal organizational approval committee.
- Committee will include professionals in fields of
  - medicine;
  - data analysis;
  - privacy;
  - information security or data protection; and
  - law and bio-ethics;
  - Including public representatives.
- The Ministry of Health shall establish a national committee
- The National Committee is authorized to decide on
  - The establishment of a central database to collect health information from several organizations.
  - Application to a data transfer outside the organization premises.

Approval mechanism (2/2)

- **The internal committee will review**
  - The purpose of the research;
  - The health field for which the data relates to;
  - The risk to data subjects privacy;
  - The researcher's professional competence; and
  - Skills and ability to meet information security and cyber requirements.
  - The expected or probable social or health outcomes of the research, and in particular, its impact on a defined group of data subjects.
- **The internal committee will state in its decision**
  - The research data description and scope;
  - The de-identification method;
  - The Identity of authorized users;
  - The data access method.
- Permit granted by the committee shall be time-limited.
- The Committee shall document the decision and retain it seven years after the completing of the research.

Anonymization (1/7)

- A process to reduce the patient identification risk while retaining the essential data for conducting the requested research.
- Organization must adopt de-identification method relevant to the type of information and the purposes of the request, following the estimated risk to privacy.
- Organization shall conduct its <u>privacy risk assessment</u>, considering the following
  a. Number of data subjects;
  b. The type and extent of data;
  c. The health field and data sensitivity;
  d. The existence of other databases the researcher can access or poses;
  e. The identity of the researcher, nature of his activity and use purpose;
  f. Number of researchers authorized users;
  g. Access requested methods, privacy and InfoSec measures;
  h. The application of the Israeli law on the applicant.

Anonymization (2/7)

- Health organization shall perform anonymization practice in consideration with the best professional methods available at that time.
- Anyone who acts by the instructions of the de-identification guidance document shall be deemed to comply with the anonymization requirement.
- For this purpose **Guidance Document** regarding anonymization means
  - An official standard (Israeli or international) as defined in the standard law 5713-1953; or
  - Reference document approved by the Ministry of Health General Director
- The Health Ministry will publish de-identification guidance documents on its website.
- The internal committee shall not authorize the creation of a re-identification key unless it convinces that there is a high likelihood that the health organization will require it to achieve its intended research use or provide medical care.
- The health organization shall not disclose the re-identification key to the researcher or any party outside the health organization.

Anonymization (3/7)

Ministry of Health de-identification Draft Guideline

Anonymization process will include at least three steps

1) Determine the extent of the minimum information required for the requested research;
2) Remove all identifying fields;
3) Perform a risk mitigation procedure on identifiable data.

Step 1 - Determine the extent of the minimum required information

- Purpose of requested use
- Description of the population about which the information
- Scope of information required
- Required information fields
- Resolution is required for each information field
- Sensitivity required

Anonymization (4/7)

Ministry of Health de-identification Draft Guideline

Step 2 - Remove all identifying items, including

ID numbers	In cases where cross-referencing of data from multiple databases is required, the organization will be allowed to pseudonymized in favor of performing the cross-referencing as an alternative to removing the ID's.
Other identifying numbers	Such as resident number, passport, driver's license, business license, insured number, medical file number, hospitalization number, prescription number.
Personal names	Such as first name and family, father's name, mother's name, children's names.
Contact Information	Such as residential address, telephone number, fax number, email address, URL, and IP address.
Passwords and payment information	Such as patient site password, operating system password, bank account number, credit card number, credit card identification numbers.
Identification numbers of equipment	Such as vehicle number, medical device identification number.

If the researcher requires to use an identifiable item, the organization needs to address this in the context of the risk management process and obtain the internal Committee justified approval. In such a case, the health organization must pseudonymized the individual ID in order to reduce the risk of immediate detection.

Anonymization (5/7)

Ministry of Health de-identification Draft Guideline

Step 3 - **De-identification of identifiable fields** – Access to Health Data within the premises of Health organization

De-Identification Model: Adjusting the de-identification techniques with respect to different field types

Field type	Description	De-identification method
Geographic items	Such as a residential address; Postal Code; Name of settlement; A hospital name; Coordinates	Shall be **aggregated**. Thus, a location can be aggregated for a district, city, or postal code, with the widest inclusion being prioritized to enable the required use of information. An alternative option, is the adding noise to the geographic data (**perturbation)**, regularly or randomly.
Dates	Such as a date of birth; Immigration; demise; hospitalization; Visitation; Treatment	Can be done in a number of ways, at different aggravation levels and according to their required use. **a.** **Generalization** - Include only a year date (exact month and day removal); **b.** **Conversion** - Converts a date with a number that represents a distance from a reference point (convert dates to days numbers from the first visit to the hospital; **c.** **Perturbation** – adding constant regularly or randomly.
Demographics and other associated details	Such as age; religion; nation; origin; native language; marital status; state of birth; occupation; educational institution; years of education; income	Can be de-identified by different methods, depending on the required usage nature. In most cases, this information will be de-identified by **pseudonymization**, **generalization**, **noise addition** or **permutation**.

Anonymization (6/7)

Ministry of Health de-identification Draft Guideline

Field type	Description	De - identification method
Structured clinical and administrative information	Such as diagnoses and coding diagnoses; Medical procedures; Clinical findings and test results; Prescriptions	It is not required to de-identified clinical data if it is necessary to realize the research. However, clinical data may be identifying or identifiable. Therefore, to the extent that some clinical data fields are not needed, they should be removed; To the extent that an organization can establish one or more of the techniques described above on clinical data without adversely affecting the study, it should address this.
Unstructured free text	Free text can often contain identifying or identifiable information, such as names, contact information, dates, or addresses.	Different methods must be explored to address this challenge, such as a. using data without giving the researcher the ability to view the data itself; b. using NLP tools to identify and remove identifying information; c. making structured and incoherent information, structured; or d. combining these methods. Often, the health organization will require to examine the data models before the researcher can access it in favor of making sure that they do not contain any identified information.
Image files	Such as photographs; X-ray imaging; MRI	Threshold requirements for de-identified image files a. Remove identifying information from the metadata (including exact dates, serial number); b. Make sure images do not contain a face image, and at least blur the image; c. Remove identifiable data embedded in the image (including the patient's name, ID, doctor's name, or date).

Anonymization (7/7)

Ministry of Health de-identification Draft Guideline

Step 3 - De-identification of identifiable fields – Transfer of health data out of health organization premises

Determination of the de-identification method according to risk management

Data type	De-identification method
Unstructured Data	Cannot be transferred, unless at the discretion of the Committee the health data adequately de-identified
Structured Data	**K – Anonymity (level of generalization)** method must be used as described 1) Organization must calculate K anonymity value for all identifiable structured fields, except for fields which contain clinical information necessary for the research; 2) A minimum threshold of **K=4** must be met, and **K=8** in cases where the level of re-identification risk is high; 3) In cases that the organization cannot reach the minimum required K value without materially adversely affecting the research purpose, it is necessary to consider subject to risk management whether there is a justification for a lower K. In these cases, the researcher must elaborate to the National Committee on the reasons for requesting health data transfer instead of access to it and why it necessary to settle for a less than required K value.

It should be emphasized that a decision on the transfer of data out of the health organization premises will be made not only by complying with the required K value, but more broadly, given the de-identification method and the various protection circuits and in accordance with the risk management performed.

Researcher obligations

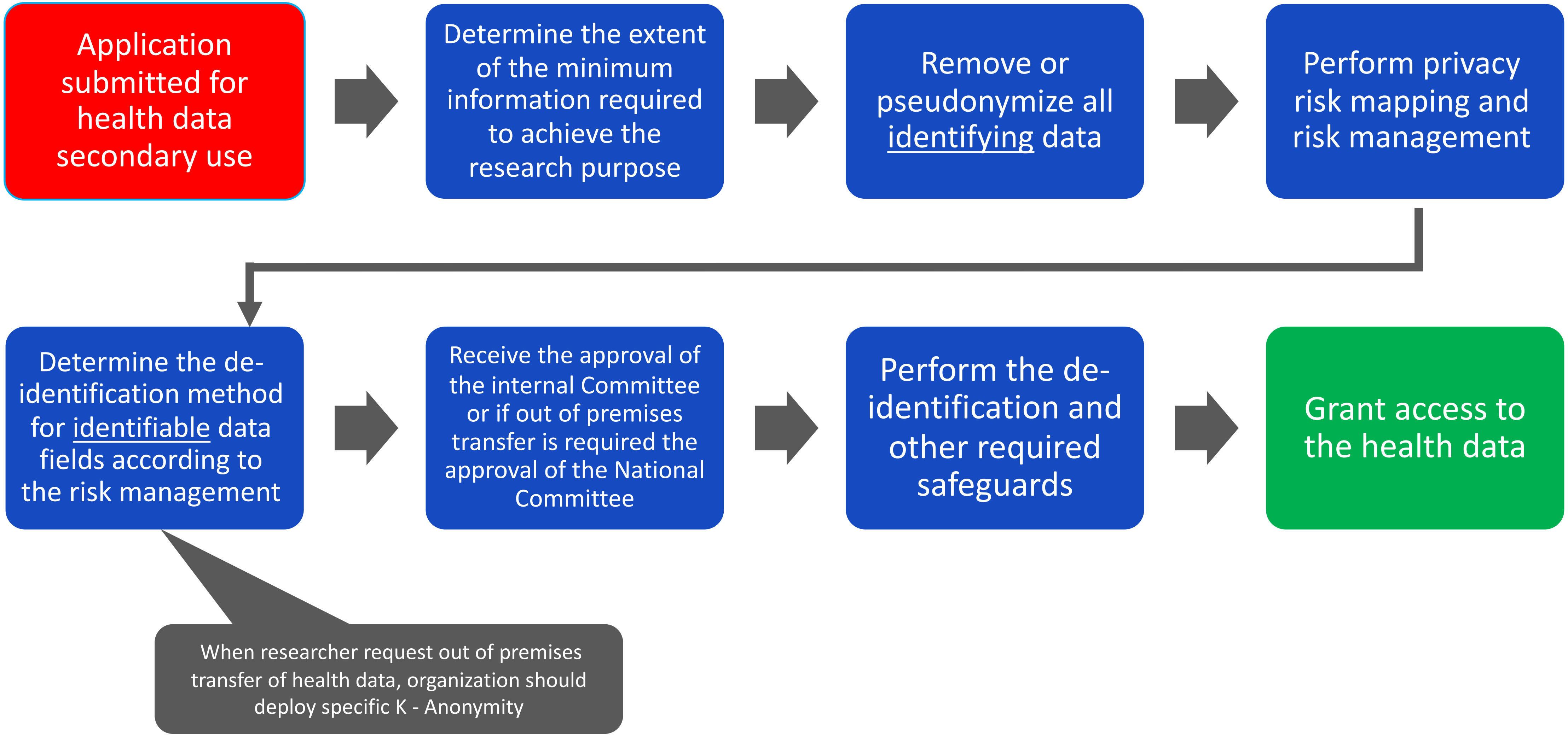
- Shall maintain confidentiality and information security;
- Shall use data only for medical research and according to the approval;
- Shall not re-identify the data;
- Shall not further transfer the data;
- Shall destroy any data that enables identification with undue delay;
- Shall report the health organization and the Ministry of Health about its infringement of the regulations or violation of the internal committee approval;
- Shall timely notify the completion of the research to the internal committee.

Data access / transfer principles

- Provide anonymized data to researchers in a secure research environment controlled by the health organization - as opposed to being transfer out of the organization premises.
- National Committee can allow to transfer health data outside the health organization premises only for exceptional, justified circumstances under all of the following conditions.
- However, transfer can only be allowed inside Israel's geographic borders. This is still under consideration

1. The applicant is a resident of Israel or a corporation registered in Israel;
2. There are technological or research limitations that do not allow a reasonable effort to perform research within the health organization premises.
3. The research may greatly benefit the individual or public health, or make a significant contribution to the advancement and improvement of medicine or medical research;
4. The external researcher possesses unique technological or research capabilities without which it is impossible to achieve the research objectives;
5. The external investigator possesses information security and privacy measures that meet the requirements set in the regulations;
6. No basis to fear that the researcher will misuse the anonymized data. A professional opinion is required to support this.

Process summary



Application submitted for health data secondary use

Determine the extent of the minimum information required to achieve the research purpose

Remove or pseudonymize all identifying data

Perform privacy risk mapping and risk management

Determine the de-identification method for identifiable data fields according to the risk management

Receive the approval of the internal Committee or if out of premises transfer is required the approval of the National Committee

Perform the de-identification and other required safeguards

Grant access to the health data

When researcher request out of premises transfer of health data, organization should deploy specific K - Anonymity

To be continued..