EUROPEAN MEDICINES AGENCY
SCIENCE MEDICINES HEALTH

Electronic Health Record: Access, Share, Expand Project

Secondary use of healthcare data; groundwork for Q&A

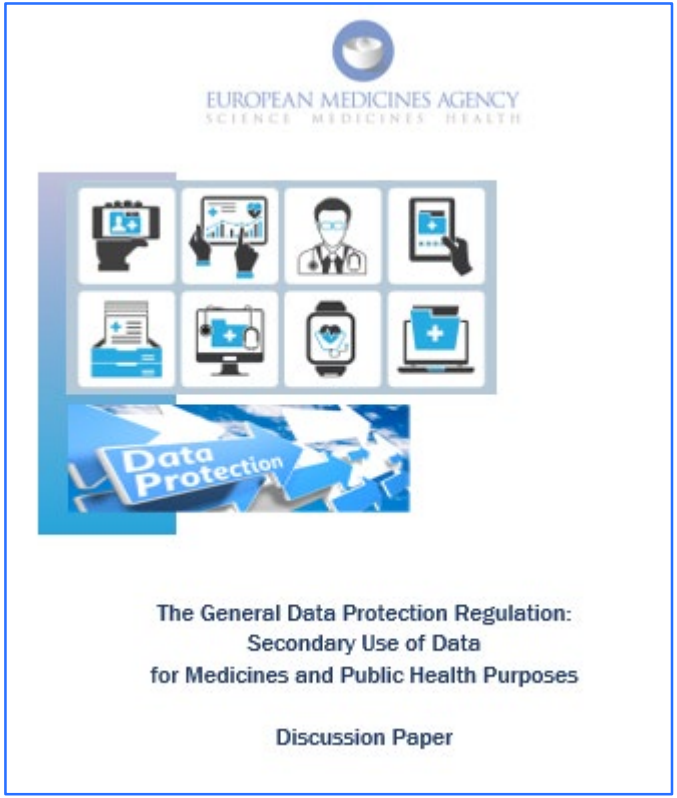
Joint PCWP and HCPWP virtual meeting, 2 June 2020

Orsolya Eotvos, Assistant Data Protection Officer, Legal Department &
Sabine Brosch, Data Protection Coordinator Clinical Studies and Manufacturing Task Force (TCS)

An agency of the European Union

Data Protection Topics

1. Secondary use of health data
2. Compatibility
3. Legal basis
4. Pseudonymisation
5. Data retention
6. Transparency
7. Data subject's rights
8. Registries
9. International Transfers



GDPR and Health Data

- **Personal data concerning health** should include all data pertaining to the health status of a data subject which reveal information relating to the **past, current or future physical or mental health** status of the data subject:
  - ✓ Information about the natural person collected in the course of the registration for, or the provision of, health care services to that natural person;
  - ✓ A number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes;
  - ✓ Information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples;
  - ✓ Any information on e.g., a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test.

GDPR and Secondary Use of Health Data

- **Processing for a compatible secondary purpose***
  - Processing of personal data for purposes other than those for which the personal data were initially collected (original, primary purposes) should be allowed **only** where the processing is **compatible** with those original purposes.
  - **No separate legal basis** (other than that which originally allowed the collection of the personal data) is required.

* See Recital 50 of the GDPR

GDPR and Secondary Use of Health Data

Processing for a compatible secondary purpose

The following should be taken into account, inter alia:

- any **link** between the **original, primary purposes** (for which the personal data have been collected) and the **secondary purposes** of the intended further processing
- the **context** in which the personal data have been collected: relationship between data subjects and the controller, the reasonable expectations of data subjects
- the **nature** of the personal data: data concerning health is a special category!
- the **possible consequences** of the intended further processing for data subjects
- the existence of **appropriate safeguards**, e.g. encryption or pseudonymisation of data further processed

GDPR and Secondary Use of Health Data

- Processing is necessary for the **performance of a task carried out in the public interest** or in the **exercise of official authority vested in the controller**

Union or Member State law may determine and specify the tasks and purposes for which the further processing should be regarded as compatible and lawful.

- Further processing for **scientific research purposes** are considered to be compatible lawful processing operations.
- The **legal basis provided by Union or Member State law** for the processing of personal data may also provide a legal basis for further processing.

GDPR - Legal Basis for Processing Personal Data

Processing shall be lawful only if and to the extent that at least one of the following applies [Article 6(1)(a)-(f) GDPR]:

a) the data subject has given **consent** to the processing of his or her personal data for one or more specific purposes

b) processing is necessary for the **performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract

c) processing is necessary for **compliance with a legal obligation** to which the controller is subject

d) processing is necessary in order to **protect the vital interests** of the data subject or of another natural person

GDPR - Legal Basis for Processing Personal Data

e) processing is necessary for the **performance of a task carried out in the public interest** or in the exercise of official authority vested in the controller;

f) processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

At any rate the existence of a legitimate interest *needs careful assessment* including *whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place*.

GDPR - Processing of data concerning health (or other special categories of data)

Prohibited, unless specific conditions are fulfilled, for example:

- **Explicit consent** to the processing of those personal data for one or more specified purposes;
- To protect the **vital interests** of the data subject or another natural person - where the data subject is physically or legally incapable of giving consent
- Reasons of **public interest in the area of public health**, such as protecting against serous cross-border threats to health or **ensuring high standards of quality and safety** of health care and of medicinal products or medical devices (on the basis of Union or Member State law).

GDPR - Pseudonymisation

- The principles of data protection apply to any information concerning an **identified or identifiable natural person**.
- Pseudonymisation means that personal data is processed in a manner that it can **no longer be attributed to a specific data subject without the use of additional information** (e.g. when a patient identification number is allocated to patients instead of using their other identifiers).
- This additional information (i.e. the code to identify the data subject) **must be kept separately and securely**.

GDPR - Pseudonymisation

The GDPR further clarifies that:

- To determine whether a natural person is identifiable, account should be taken of all the **means reasonably likely to be used**, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly.
- Account should be taken of all **objective factors**, such as:
  - the **costs** of and the amount of **time required for identification**,
  - taking into consideration the **available technology** at the time of the processing and
  - **technological developments**.

GDPR - Pseudonymisation ≠ Anonymisation

- The **principles of data protection do not apply to anonymous information.**
- What is anonymous information?
  - Information which **does not relate to an identified or identifiable** natural person or to personal data rendered anonymous in such a manner that the data subject is **not or no longer identifiable**.
  - The GDPR does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

GDPR and Data Retention ('storage limitation')

- Personal data should be kept (in a form which permits identification) for **no longer than is necessary for the purposes** of the processing.
  - ➢ The period for which the personal data are stored should be strictly limited: time limits should be established for **erasure/anonymisation** or for **a periodic review**
- The retention period should correspond with the purposes and the legal basis: for example, if consent is withdrawn, data is to be deleted unless **further retention is necessary**, e.g.
  - ✓ for compliance with a legal obligation
  - ✓ for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
  - ✓ on the grounds of public interest in the area of public health
  - ✓ for scientific research purposes or statistical purposes

GDPR and Transparency

- The GDPR states that personal data should be processed **lawfully, fairly and in a transparent matter.**

➢ It should be transparent to the data subject as a natural person that his or her **personal data are collected, used, consulted or otherwise processed**.

➢ Principle of transparency requires that any **information and communication** relating to the processing of personal data is:

  ➢ easily accessible;
  ➢ easy to understand;
  ➢ clear and plain language is used when providing such information.

Privacy Statements, Data Protection Notices

GDPR and Transparency

Data subject is entitled to obtain information regarding:

- Identity, contact details of the **controller** and the **data protection officer**
- **purposes** as well as the **legal basis** of the processing
  - The specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data
- **Further information** to ensure fair and transparent processing, such as
  - Categories of data processed, the recipients of data (outside of EU/EEA?)'
  - The retention period or the criteria to determine such period,
  - The risks, rules, safeguards and rights in relation to the processing of personal data
  - How to exercise their rights and lodge complaints regarding the processing.

GDPR and Rights of the Data Subject

- **Right of access** to personal data which have been collected: data subjects should have the right to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing;
  - This includes the right for data subjects to have **access to data concerning their health**, for example the data in their medical records containing information such as diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided;
- Controller should use all reasonable measures to **verify the identity** of a data subject who requests access
  - But a controller should not retain personal data for the sole purpose of being able to react to potential requests.

GDPR and Rights of the Data Subject

- **Right to rectification**: Data subjects have the right to have inaccurate or incomplete personal data concerning them rectified or completed without undue delay.
- **Right to be forgotten:** to have personal data erased and no longer processed if
  - they are no longer necessary in relation to the purposes they processed,
  - the data subject has withdrawn his or her consent or objects to the processing,
  - the processing of personal data does not otherwise comply with the GDPR.
- Data must be deleted unless **specific conditions** apply (see examples for further retention)

GDPR and Registries

"By **coupling information from registries**, researchers can obtain **new knowledge of great value** with regard to widespread medical conditions such as cardiovascular disease, cancer and depression. On the basis of registries, **research results can be enhanced**, as they draw on a larger population. […]

Research results obtained through registries provide solid, high-quality knowledge which can provide the basis for the formulation and implementation of **knowledge-based policy**, improve the quality of life for a number of people and improve the efficiency of social services.

In order to facilitate scientific research, personal data can be processed for scientific research purposes, subject to appropriate conditions and safeguards set out in Union or Member State law." Recital 157 of GDPR (emphasis added)

GDPR and International Transfers

- Special safeguards are foreseen to ensure that the protection travels with the data when personal data is transferred outside the EEA.
- GDPR offers different mechanisms to achieve this, such as:
  - **Adequacy decisions**
  - **Standard data protection clauses** (adopted by EC or national supervisory authority)
  - **Binding corporate rules**
  - **Certification mechanism and codes of conduct**
  - **Contractual clauses (between controller-processor)***
  - **Legally binding and enforceable instrument between public authorities or bodies**
  - **Provisions for administrative arrangements between public authorities and bodies***

** Subject to the authorisation of the competent national supervisory authority*

GDPR and International Transfers

In the absence of the abovementioned mechanisms, the GDPR allows **derogations for special situations**:

- The data subject has given his or her **explicit consent** to the transfer
- The transfer is necessary for the performance of a **contract or establishment of a legal claim**
- The transfer is necessary for **important reasons of public interest** or
- The transfer is necessary to **protect the vital interests** of the data subject or of other persons (where the data subject is physically or legally incapable of giving consent)
- The transfer is **made from a register established by law** and intended for consultation by the public or persons having a legitimate interest.

Where none of the above is available: transfers qualified as not repetitive and that only concern a limited number of data subjects, could also be possible for the purposes of the compelling legitimate interests pursued by the controller (see Recital 113 of GDPR)

Stakeholder Consultation

- EMA is consulting interested stakeholders in parallel
  - On 3 March, PCWP and HCPWP were invited to express interest to provide input in the drafting of the Q&As
- For the consultation, interested stakeholders are grouped in two categories:
  - **Patients and consumers** as data contributors and
  - **Medicines developers, research performing and research-supporting infrastructures** and other data providers (e.g., prescribing and dispensing data)
- EMA circulated **discussion papers** on 12/13 May to obtain input on data protection questions from the two stakeholder groups.

Any questions?

Further information

Sabine.Brosch@ema.europa.eu; Orsolya.Eotvos@ema.europa.eu

Official address Domenico Scarlattilaan 6 ● 1083 HS Amsterdam ● The Netherlands
Address for visits and deliveries Refer to www.ema.europa.eu/how-to-find-us
Send us a question Go to www.ema.europa.eu/contact **Telephone** +31 (0)88 781 6000

Follow us on **@EMA_News**