FABIAN PRIVACY LEGAL

# Data privacy considerations in clinical trial disclosures under EU laws

**Daniela Fábián Masoch,** Founder FABIAN PRIVACY LEGAL

Pharmaceutical Compliance Congress and Best Practices Forum

May 10 – 12, 2016, Warsaw, Poland

## Protecting the privacy of research participants

Legal framework and standards (selection)



- EMA policy 0070 on publication of clinical data — January 2015
- EMA policy 0043 on access to documents — December 2010
- EMA Guidance on the anonymisation of clinical reports for publication purposes (EMA 0070) — March 2016
- EU Regulation on data protection 45/2001/EC (Community Institutions and Bodies)
- EU Directive 95/46/EC on data protection
- EU GDPR (published on May 4, 2016)
- WP29 opinion on anonymisation techniques (April 2014)
- ICO Code of Practice on anonymisation (November 2012)

## Key data privacy considerations for companies

3

- Companies must:
  - Comply with data protection rules when disclosing clinical trial data and protect the privacy of research participants and other individuals participating in the clinical study
  - Balancing the protection of patient's privacy (anonymisation) while retaining a maximum of scientific useful data for research purposes
  - Take responsibility for anonymising patient data prior to publication while retaining a maximum of useful information
  - Ensure that it is not "reasonably likely" that anonymised data will lead to re-identification of individuals when matched with data available elsewhere
  - Conduct a privacy impact assessment to identify the possibility and likelihood of re-identifying the data by someone using all reasonable steps
  - Require consent and/or anonymise the patient level data



FABIAN PRIVACY LEGAL

## Definitions

4

| | |
|---|---|
| Personal data | • Any information relating to an identified or identifiable natural person (a person is identifiable either directly or indirectly, such as by reference to a code) |
| Anonymisation | • Process on personal data to render it "irreversibly" no longer identifiable<br>• Re-identification through combination with other data is not likely to take place by using all the means likely reasonably to be used by either the controller or a third party<br>• Anonymised data is not personal data |
| Pseudonymization | • Process on personal data to render it no longer attributable to a specific individual without use of additional information that is kept separately and is subject to technical and organizational measures to ensure non-attribution: replacing one attribute by another (key-coding of patient data)<br>• Pseudonymised data is still personal data |
| Consent | • Specific, freely given, informed and unambiguous (for sensitive data explicit) indication of agreement to the processing of personal information |



FABIAN PRIVACY LEGAL

## Anonymisation requirements

5

- Anonymisation of personal data is further processing of the data and subject to data protection laws
  - General privacy principles apply
  - Legitimate basis for anonymisation (consent / legal obligation, legitimate interest)
  - Right to object on compelling legitimate grounds relating to the particular situation to the processing of personal data – if justified, no further processing
- WP29 considers anonymisation process as a form of compatible further use of personal data
- Consent to anonymise personal data is not required if:
  - Anonymisation does not result in distress or damage to the individual
  - The purpose of anonymisation is legitimate
  - Individuals have been informed about the process and the use of data
  - Procedure to handle legitimate objections are in place



## Anonymisation criteria

6

- Effective anonymisation of personal data is reached when the following criteria are met:
  1. It is not possible to single out an individual in a dataset
  2. It is not possible to link records relating to an individual within a dataset or between two separate datasets
  3. Information cannot be inferred concerning an individual in a dataset **OR**
  4. Whenever **one** of these 3 criteria is not met, through an evaluation of the risk of re-identification

## Anonymisation techniques

7

- Anonymisation shall be based on a combination of several techniques with the goal to strip off sufficient identifiers so that the individual can no longer be identified
  - Removal or masking through generalisation or randomisation of
    - Direct identifiers (such as name, e-mail, phone number, address, patient ID) and
    - Indirect identifiers such as:
      - Geographical location
      - Relative dates
      - Demographic information: sex, age, race, height, weight;
      - Dates: birth, visits, adverse events
    - Randomisation removes the strong link between data and the individual
    - Generalisation modifies for ex. date of birth with year of birth or age with an age range
  - Breaking the code to original data set



## Possible approach to effective anonymisation

8

- Information of patients
  - Anonymisation procedure for potential further processing and disclosure purposes
- Risk assessment evaluating the risk of re-identification taking into account
  - Personal data has been collected in compliance with data protection laws
  - Identification of direct and indirect identifiers
  - Feasibility of anonymisation
  - Data utility considerations
  - Risk of re-identification (establish threshold – 0 risk or very low risk: EMA 0.09%)
  - Appropriate measures are in place to avoid re-identification (contract)
- Selection of appropriate anonymisation techniques
- Documentation of anonymisation methodology and process (managing risk of re-identification or demonstrating that all three criteria are met)
- Redaction of personal data of investigators, sponsors, staff etc.