GDP What?
How the European Union General Data Protection Regulations Impact Research

Robyn Shapiro, JD
Founder
Health Science Law Group LLC

Karen Hartman, MS, CHRC
Division Chair
Research Administration
Mayo Clinic

©2019 MFMER | slide-1

Objectives

- Review the scope of GDPR and impact to research.
- Identify best practices for implementation.
- Share practical considerations through case study discussions.

©2019 MFMER | slide-2

GDPR Overview

- Applies to organizations worldwide that process (collect, use, store, and/or transfer) personal data about individuals in the EEA, where the organization's processing activities are related to:
  - (a) the offering of goods or services to individuals in the EEA, or
  - (b) the monitoring of individuals' behavior within the EEA.
- Effective May 25, 2018

©2019 MFMER | slide-3

GDPR Overview

- Not limited to health data or PHI. GDPR "Personal Data" includes ALL data about identified or identifiable natural person including:
  - web data such as browsing behavior, location, IP address, cookie data and RFID tags.
  - health, biometric and genetic data.
  - de-identified information (under HIPAA) that is not anonymized.
  - consumer/purchase information.
- Significant financial penalties for non-compliance (4% of gross revenue or 20 million Euros, whichever is greater).

©2019 MFMER | slide-4

Scope

- GDPR applies to:
  - Organizations anywhere in the world that process the personal data of those in the EEA related to offering of goods and services, regardless of whether payment is exchanged.
  - Organizations anywhere in the world that monitor the behavior of subjects as far as their behavior takes place in the EEA.

©2019 MFMER | slide-5

Definitions

- **Personal Data**: *Any information relating to an identified or identifiable natural person ("data subject"). GDPR, Art. 4(1).*
- **Controller**: *The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. GDPR, Art. 4(7).*
- **Processor**: *A natural or legal person, public authority, agency or other body which processes EU Personal Data on behalf of the Data Controller. GDPR, Art. 4(8).*

©2019 MFMER | slide-6

Definitions

- **Anonymized**: *Information which does not relate to an identified or identifiable natural person or personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. 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. Recital 26.*
- **Pseudonomized**: *Personal data that can no longer be attributed to a data subject without the use of additional information. The additional information must be kept separately subject to technical and organizational measures to ensure non-attribution to an identified or identifiable living person. GDPR, Art. 4(5).*

©2019 MFMER | slide-7

Applicability of Scope

- Applies to European Economic Area (EEA).
  - Comprised of the 28 EU member states and Iceland, Liechtenstein and Norway.
  - EU member list:
    - *Austria, Belgium, Bulgaria, Croatia, Czech Republic, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, United Kingdom.*
  - Note: will still apply in the UK despite Brexit

©2019 MFMER | slide-8

Applicability to Research

- What about research and impact to Universities and Academic Medical Centers?
- Think beyond PHI to personal data
  - Clinical research projects (trials, datasets, collaborations).
  - Staff members - personal data for access to sponsor systems.
  - Education and training activities.

©2019 MFMER | slide-9

When can GDPR Apply for AMC:

- Established entity in the EEA - acts as a data controller or processor.
- Offering goods or services to individuals in the EEA (telehealth, targeting or specific marketing for clinical trials).
- Monitoring the behavior of individuals in the EEA (remote data for clinical care or research use captured and sent to US).

©2019 MFMER | slide-10

GDPR application - Examples

- Online education (professional development credit program, etc.).
- Recruiting students from EEA member states.
- Recruiting or marketing to patients in the EEA.
- Offering telemedicine services to patients in the EEA.

©2019 MFMER | slide-11

GDPR application - Examples

- Sponsoring clinical research with a site located within EEA member states. Identify data movement for responsibilities.
- Direct awardee (or sub) through EEA institutions of European governmental grants or contracts to perform research services.
- Serving as a core data center or lead site for a multi-national clinical trial with EEA-based sites.

©2019 MFMER | slide-12

Implementation Plans

- Gather stakeholders
  - Consider Legal, Compliance, Information Technology and Security, System Owners, Contracting, Institutional Review Board and others that may be impacted.
- Conduct an analysis of GDPR impact to specific areas. Risk rank based on impact, volume and likelihood.

©2019 MFMER | slide-13

Research Analysis

- Does it apply?
  - Who are the participants?
  - Where are the data collected?
  - Data flow mapping is important for identifying likelihood and impact.
    - Where does the data come from and where does it go?
    - Identify the systems that contain “GDPR data”?

©2019 MFMER | slide-14

Broad scope

- Contracting
  - Are any addendums needed?
- IRB
  - Any consent form changes (template) or consent form addendums needed?
- Communications
  - Researchers, support staff, broader community.
  - Identify a point of contact for research.

©2019 MFMER | slide-15

Legal

- Interpretation of GDPR and applicability to Institutional work.
  - Need coordination between Clinical (practice), Compliance, Privacy Office, Marketing, Laboratory, Research and Education (not all encompassing).
  - Recognize other organizations may differ from own interpretation in what they consider “applicable under GDPR.”

©2019 MFMER | slide-16

Analysis of Impact

- Contracts
  - Identify lists of collaborators and sponsors.
  - Review volumes for collaborations.
  - Identify AMC role: controller or processor?
  - Determine risk based on volumes and data flow.
- Grants
  - Any EU grants (prime or sub)?
  - Any subs on NIH/federal awards? Where does data flow?

©2019 MFMER | slide-17

Analysis of Impact

- Institutional review Board
  - Identify studies with multi-national sites. Is the AMC/PI the sponsor?
  - General volume determination for risk.
  - Review consent form templates for potential changes.
  - Identify if policies and/or procedures need updating.
  - Communication, education and training.
    - Awareness is key!

©2019 MFMER | slide-18

Analysis of Impact

- Systems and Data
  - Identify where EEA participant data may exist.
  - Clinical trial systems? Survey data systems? Other datasets maintained by researchers?
  - Determine (if possible) risk related to volume and percentage of data.
  - Data mapping considerations:
    - How to obtain? Who has access? Can you track the data flow and movement?

©2019 MFMER | slide-19

Analysis of Impact

- Website
  - Are you targeting (or marketing your research) in a specific country within the EEA?
  - Any websites or documents translated for EEA members?
- Clinical sites within the EEA referring patients to the US for clinical trials?
- Education or training
  - Are Continuing Professional Development classes translated into other languages?

©2019 MFMER | slide-20

Practical Considerations

- Deletion Requests
- Risk analysis
  - What % of the data “may” be from an EEA patient? Where was it collected?
- Contact for participants if they have questions?
- Who will be the Data Protection Officer? Can you use another individual within research as the point of contact?
- Breach notification process
- If needed, an institutional EEA representative appointment.

©2019 MFMER | slide-21

Case study 1

- Academic Medical Center in the US is participating as a site in a multi-national investigational device study. The sponsor’s headquarters are in the EEA. All participants at the AMC site are from the US.
  - Data is entered in an Electronic Data Capture (EDC) system for the sponsor to review and monitor.
  - Study staff provide credentials, including email, name, role and birth month/year for access to the system.

©2019 MFMER | slide-22

Case study 1

- Let's discuss….
  - GDPR applicability?
  - Discussion and considerations for the AMC site.
  - Operational impacts for study staff?

©2019 MFMER | slide-23

Case study 2

- Academic Medical Center in the US is the sponsor of a single US site, prospective clinical trial.
  - Study involves an investigational drug (monthly infusion) with participant completing QOL questionnaires bi-weekly via a web based system.
  - Participant #10 travels to Paris on vacation and completes the questionnaire from her hotel room.
  - Data is transferred via the system to the US site.

©2019 MFMER | slide-24

Case study 2

- Lets discuss…
  - GDPR applicability?
  - Discussion and considerations for the AMC site and this particular participant or future participants.

©2019 MFMER | slide-25

Case study 3

- A university in an EEA country is sending tissues samples under an Material Transfer Agreement to a US Academic Medical Center.
- The US AMC will perform research diagnostic genetic analysis. The EEA University retains ownership of the samples.
- Joint publications are planned based on the results.

©2019 MFMER | slide-26

Case Study 3

- Lets discuss…
  - GDPR applicability?
  - Parties roles?
    - EEA University role?
    - AMC US University role?
  - What needs to be considered?

©2019 MFMER | slide-27

Case study 4

- The same EEA university is now sending waste tissues samples to the US Academic Medical Center.
- No data accompanies the samples.
- The US AMC will perform research on the samples.

©2019 MFMER | slide-28

Case Study 4

- Lets discuss…
  - GDPR applicability?
  - Parties roles?
    - EEA University role?
    - AMC US University role?
  - What needs to be considered?

©2019 MFMER | slide-29

Questions & Discussion

©2019 MFMER | slide-30

Contact Information

- Karen Hartman
  - Phone: (507) 538-5238
  - Email: hartman.karen@mayo.edu
- Robyn Shapiro
  - Phone: (414) 206-2101
  - Email: Robyn.Shapiro@healthscienceslawgroup.com

©2019 MFMER | slide-31