



FOUNDED BY BRIGHAM AND WOMEN'S HOSPITAL
AND MASSACHUSETTS GENERAL HOSPITAL



Overview of the European Union General Data Protection Regulation for the Partners Research Community

May 2018

Introduction

This slide deck provides a high-level overview of the European Union (EU) General Data Protection Regulation (GDPR) for the Partners research community.

The deck includes:

- PI “Take-Aways” – what to look for in the slide deck
- General Background on EU Data Protection Laws
- Countries Subject to the EU GDPR
- PI and GDPR Compliance Requirements
- Crosswalk Between HIPAA and GDPR
- Key GDPR Definitions
- Scenarios
- Information on Required Subject Disclosures and Consent Requirements
- Breach Notification
- Recap
- Where To Go for Help
- Acknowledgements

PI “Take-Aways”

- The GDPR adds an element of complexity to collaborations with EU institutions.
- Familiarize yourself with the basic GDPR requirements outlined in this slide deck prior to collaborating with an EU colleague/institution or when receiving personal data from the EU.
- Follow the GDPR instructions of the Pre-Award team during the application/proposal development/submission process.
- Follow GDPR instructions from the relevant contracting office during negotiation of a research contract or data use/material transfer agreement.
- To comply with GDPR requirements, you may have to modify lab/research group work flows, processes, record keeping, etc.
- Report known or suspected GDPR data breaches immediately to the hospital’s Privacy Office for investigation by the Privacy Office/Information Security and institutional reporting, if necessary.

Current Situation re: EU Data Protection Laws

- The GDPR replaces existing EU privacy laws. It expands personal privacy rights for EU residents and non-EU residents located in the EU.
- It applies not only to EU institutions but also to institutions *with no physical EU presence*, e.g., a Partners hospital, if that institution works with what the regulation defines as Personal Data.
- There are correlations between HIPAA and GDPR, but the GDPR is broader, extending to areas and information not covered by HIPAA.
- Enforcement begins May 25, 2018 and will affect Partners research collaborations with EU entities. For example:
 - EU hospitals acting as clinical trial sites or data coordinating centers under a Partners project, or
 - EU universities collaborating on a Partners hospital basic science project.

Penalties for non-compliance are significant: up to €20,000,000 or 4% of the total worldwide annual turnover of the preceding financial year, whichever is greater.

The landscape is changing rapidly



- Despite the 5/25/18 enforcement date, the definitions of many GDPR terms are still under discussion with frequent new guidance documents released by the EU with new interpretations and compliance requirements.
- While the GDPR is intended to bring consistency to EU member state privacy laws, EU member states still have significant authority to interpret GDPR language and implement additional requirements.
- Partners research offices (Research Management, Clinical Trials Office (CTO), Innovation, Human Research Affairs) are working with the Office of General Counsel, Information Security and Privacy, and Research Compliance to keep abreast of the shifting landscape and provide up-to-date information to the research community.

Countries Subject to the EU GDPR

- The EU GDPR applies to the European Economic Area that includes the EU and Iceland, Liechtenstein, and Norway. The EU includes the following 28 countries:

Austria	Italy
Belgium	Latvia
Bulgaria	Lithuania
Croatia	Luxembourg
Cyprus	Malta
Czech Republic	Netherlands
Denmark	Poland
Estonia	Portugal
Finland	Romania
France	Slovakia
Germany	Slovenia
Greece	Spain
Hungary	Sweden
Ireland	United Kingdom

Countries Subject to the EU GDPR – continued

- The list on the preceding slide is posted on the *Navigator*.
- Other nations may elect to adopt the GDPR or may have stricter data privacy laws than the US.
- We recommend PIs review this list before engaging in an international collaboration or sharing data. If you have questions, send them to CISPO@partners.org.
- We will keep the research community apprised of changes through additional *Navigator* postings and *News* items, i.e., when other countries adopt the EU GDPR standards.

What PIs Should Do: GDPR Compliance

- PIs and their staff with existing EU collaborations or contemplating entering into an EU collaboration or receiving EU data should follow GDPR announcements on the *Navigator*, Research Compliance page, <https://partnershealthcare.sharepoint.com/sites/phrmResources/c/Pages/GDPR.aspx>.
- PIs should also follow the GDPR instructions of the
 - Pre-Award team when submitting a grant application/contract proposal,
 - IRB office when submitting a protocol for review, or
 - Contracting office (CTO, Research Management, or Innovation) during the contract, subcontract, or data use/material transfer negotiation process.
- The contracting offices will work with PIs and their staff, and the Office of General Counsel and external counsel as needed, to identify GDPR compliance requirements prior to executing contracts or agreements.






What PIs Should Do: GDPR Compliance

- **GDPR compliance may require PIs to establish new processes and work flows within their labs/research groups.** For example:
 - Send GDPR notifications to EU collaborators prior to submitting a grant application or proposal,
 - Include GDPR language in consent forms used in the EU and on rare occasions in consent forms used at the Partners hospital or other US sites,
 - Give EU participants an opportunity to withdraw from a study and take certain necessary actions if/when EU participants invoke their privacy rights (e.g., right to be forgotten, right to erasure), and
 - Establish new information security requirements for storing, using, or sharing data.
- **You may not agree to any GDPR requirements in a research contract/agreement that Partners, the hospital, you and your lab/research group cannot meet.**

GDPR, HIPAA and Compliance Requirements

- The GDPR is just as technical as HIPAA and requires a very fact dependent and individualized analysis.
 - Given the changing landscape, these analyses may take time. Please be patient. It's a brave new world for all of us.
- The next slide identifies key HIPAA terms and links them to their GDPR counterparts. These terms are not exact equivalents.
- The slides that follow provide definitions of the most common GDPR terms.

Crosswalk Between HIPAA and the GDPR

<u>HIPAA Term</u>		<u>GDPR Term</u>
Covered Entity		Controller
Business Associate		Processor
Use Disclosure		Processing*
Protected Health Information		Personal Data (including Pseudonymised)
De-identified		Anonymized

* Note that special rules apply to transfers of personal data out of the EU (a particular type of processing).

GDPR Key Definition – Controller

- **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**”
- **For example**, when a Partners hospital drafts a protocol through a PI, the hospital is determining, at least in part, the purposes and means of processing of data collected in the study and is therefore considered a “controller” for GDPR purposes.



GDPR Key Definition – Processor

- **Processor** – “a natural or legal person, public authority, agency or other body **which processes personal data on behalf of the controller**”
- **For example**, a “processor” may be a Partners hospital providing research-related services such as data analysis under a PI’s direction.



Key Definition – Personal Data

- **Personal data** – any information relating to an identified or “identifiable natural person”
 - “Identifiable natural person” – a person who can be identified, directly or indirectly, **such as by an identifier** (*e.g.*, a name, **identification number**, or one or more factors specific to physical, physiological, genetic, mental, economic, cultural or social identity)
 - “To determine whether a natural person is identifiable, [consider] . . . **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.”
- **Unlike HIPAA, Personal Data are not limited to research participants and patients.** It applies to personal data of **EU-located** investigators, study staff, and other individuals.
 - For example, information a EU collaborator provides as part of the Partners grant application process: salary, bio-sketch, academic rank, other support, COI disclosure, etc. This is not limited to the PI; it includes all **EU-located** staff participating in the project.

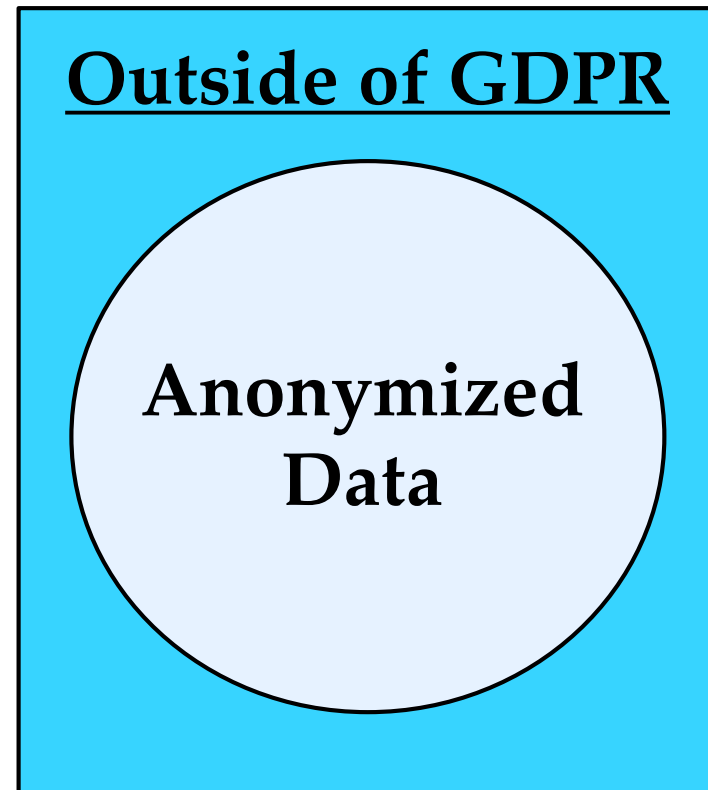
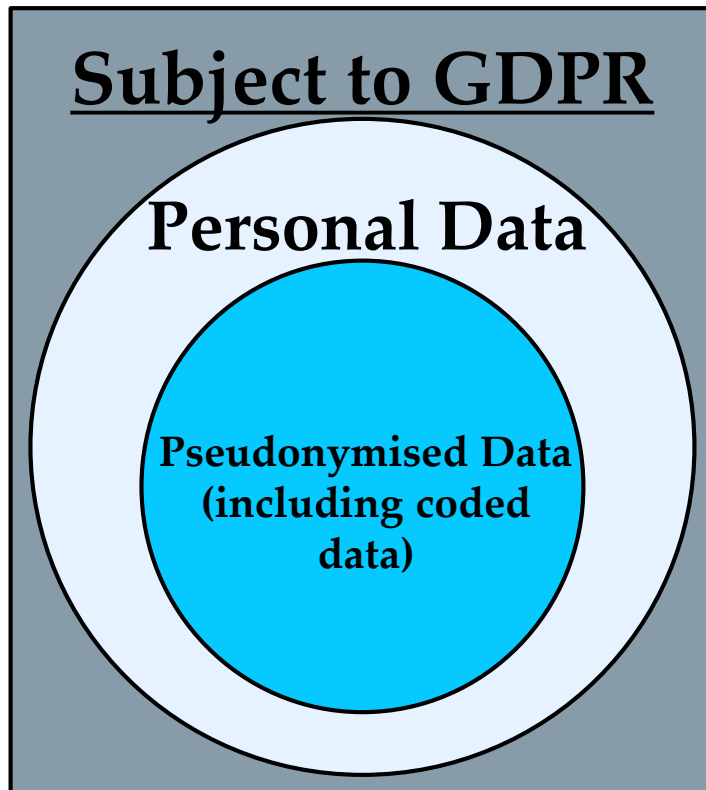
Key Definition – Pseudonymisation

- **Pseudonymisation** is the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information which is kept separate and protected. For example, coded data.
- **Under GDPR pseudonymised data, what we generally think of as coded data, must be treated as “personal data,” i.e., identifiable.** This is a big change from how coded data are treated under HIPAA.
- The GDPR does not apply to the processing of anonymous information, including for statistical or research purposes. (See next slide.)

Key Definition – Anonymization

- **Anonymization** is the process of either encrypting or removing personally identifiable information from data sets so that the individuals whom the data describe remain anonymous.
- **Anonymization is an irreversible process that removes the ability to identify the data subjects. A data set is not necessarily anonymized under the GDPR because it is de-identified under HIPAA, e.g., all HIPAA-identifiers have been removed.**
- According to Article 29, Data Protecting Working Party Opinion 05/2014, “once a dataset is truly anonymized and individuals are no longer identifiable, [the] European data protection law no longer applies.” This does not apply to coded-data.

What is Subject to or Outside GDPR



Key Definitions – Processing and Consent

- **Processing** – any operation or set of operations performed on personal data, such as collecting, recording, organizing, structuring, storing, adapting or altering, retrieving, consulting, **using, disclosing by transmission, disseminating or otherwise making available**, aligning or combining, restricting, erasing or destroying.
- **Consent** – any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

Key Definitions – Special Categories of Data

Certain data are subject to heightened protections:

- **Data concerning health** – personal data related to the physical or mental health of a natural person (including the provision of health care services) which reveal information about the individual’s health status,
- **Genetic data** – personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person **and which result, in particular, from an analysis of a biological sample from the person,** and
- **Biometric data** – personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, **such as facial images or dactyloscopic data (fingerprints).**

Processing Special Categories of Personal Data



- **Processing of the three special categories of personal data identified in the preceding slide (genetic data, biometric data for the purpose of uniquely identifying a person, and data concerning health) is prohibited.**
- **However, the GDPR does allow for exceptions. These are listed on the following slide and provide the basis for Partners research collecting and using Personal Data.**

Processing Special Categories of Personal Data: Exceptions

- The main GDPR exceptions to processing Personal Data:
 - Data subject has given **explicit consent** to the processing,
 - Processing is necessary for reasons of **substantial public interest**,
 - Processing is necessary for reasons of **public interest in the area of public health**, such as protecting against serious cross-border threats to health or **ensuring high standards of quality and safety of health care and of medicinal products or medical devices**,
 - Processing is necessary for **archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes**, or
 - Processing is necessary for the **establishment, exercise or defense of legal claims**.

Scenario 1 – Partners hospital is a site under a trial awarded to an EU institution

- MGH is serving as a site in a study **solely** developed and awarded by an industry sponsor to an EU institution. MGH, operating under a subcontract from the EU institution, will be sending subject data to the EU. No EU data will be coming to the U.S.
- Analysis
 - MGH is not providing services to or monitoring the behavior of subjects in the EU, thus **it is not directly subject to the GDPR.**
 - If MGH subject data will be sent to the EU, the EU institution may ask the MGH to revise its consent forms to comply with the GDPR so that the EU institution's processing of those data in the EU is permitted under the GDPR.

Scenario 2 – Partners hospital has received an award and is collaborating with EU entities

- BWH has received a grant that includes sites in the EU (working under subcontracts from BWH) collecting data on subjects located in the EU. Subject data will be sent from the EU to the U.S.
- Analysis
 - The BWH is monitoring the behavior of (and potentially indirectly providing research-related services to) data subjects in the EU because it is the “sponsor” of the study, thus **GDPR applies to the U.S. institution as a controller.**
 - BWH should ensure that there are bases under the GDPR that permit processing of (1) EU subject data (for various purposes, such as conduct of the study, transfer to the U.S., secondary research, etc.) and (2) EU investigator and study staff data.
 - The BWH will need GDPR-compliant privacy and security policies and procedures and may need an EU legal representative, a Data Protection Officer (who is identified to relevant EU data protection authorities), and flow-down terms in vendor contracts, etc.

Scenario 3 – Partners hospital is a site and serving as DCC for the trial

- MGH is a study site in an industry-sponsored clinical trial. Other sites for this trial include EU sites. MGH is also serving as the DCC for the study, receiving coded data from all sites, including those in the EU.
- Analysis
 - The industry sponsor is a controller under GDPR because the sponsor determines the purposes and means of processing data of EU subjects in relation to the trial.
 - MGH is a processor because as the DCC MGH is processing personal data of EU data subjects on behalf of the sponsor.
 - The personal data MGH processes includes both
 - Coded personal data of EU study participants, and
 - Fully identifiable data of EU investigators and study staff.
 - In its role as processor, MGH's key responsibilities are
 - Entering data,
 - Maintaining a record of processing activities,
 - Adopting data protection policies, and
 - Amending contracts with third parties that may have access to personal data from MGH.
 - Depending on the specific facts of the trial and the sponsor's requirements, among other responsibilities, MGH may have to designate an EU legal representative and/or appoint a Data Protection Officer.

Scenario 4 – Partners hospital receives and stores samples as part of international clinical trial

- As part of an industry-sponsored international clinical trial, TIMI is receiving and storing samples, including samples collected by sites in the EU. TIMI receives the samples in coded form. TIMI analyzes the samples in the context of the trial and sends its analysis back to the respective study sites. Following completion of the study, TIMI also maintains the samples in coded form to allow for secondary research by other researchers. The samples may be shared with researchers for secondary research with or without codes.
- Analysis
 - The industry sponsor is the controller because it determines the purposes and means of processing data of EU data subjects in relation to the trial. BWH (due to TIMI's activities) is the processor under GDPR because it is processing personal data of EU data subjects on behalf of the sponsor.
 - Coded samples by themselves are not personal data under the GDPR, but data generated through analysis of the coded sample is personal data under GDPR.
 - Secondary researchers receiving coded samples may be subject to the GDPR by contract because the data generated would be personal data under the GDPR.
 - Secondary research with non-coded and otherwise anonymized samples would not be subject to GDPR because the research does not involve personal data.

Required Disclosures to the Data Subject

- The GDPR identifies information that must be provided to the data subject in a consent form at the time the data are collected.
- The required information is similar to what would typically be included in a consent form with some GDPR-specific additions.
- **Partners is developing sample consent forms and other notifications to assist PIs in fulfilling this requirement.** When available, these will be posted on the Research Compliance page of the *Navigator*.

Required Disclosures to the Data Subject: Examples

- Controller's identity and contact information
- If appointed, Data Protection Officer contact details
- Why the personal data are being processed, including the legal basis
- Where the processing will be done and whether processing will be by the controller or a third party
- Whether the data will be transferred to a third country or international organization, the legal basis for the transfer, and how a copy may be obtained
- Storage information
- Right to request access, rectification, erasure or restriction of processing, to object to processing and the right to data portability.

Consent

- Under the GDPR a data subject's consent may be given in the context of a written document that also addresses other matters. To be valid the consent must be:
 - **Clearly distinguishable from the other matters**, and
 - Intelligible and easily accessible, using **clear and plain language**
- The data subject must have the **right to withdraw** his or her consent at any time. The withdrawal process must be as easy as the consent process.

Breach Notification

- The GDPR timeline for reporting data breaches is much shorter than the U.S. timeline.
- **In most situations GDPR breaches must be reported within 72 hours.**
- **PIs and their staff are required to notify the hospital's Privacy Office immediately upon becoming aware of an actual or potential breach.**
 - For example, loss of a laptop or flash drive that includes personal data collected from subjects located in the EU.
- The Privacy Office, with Partners Information Security, will investigate the incident to determine the nature of the breach, whether reporting does have to occur, and to whom the breach must be reported. *The PI is not authorized to make this determination.*

List of Privacy Officers:

https://pulse.partners.org/resources_training/wikis/is/is_wiki_item/privacy_contacts_by_institution

Recap

- The GDPR adds an element of complexity to collaborations with EU institutions.
- PIs should familiarize themselves with the basic GDPR requirements outlined in this slide deck prior to collaborating with an EU colleague/institution or when receiving personal data from the EU.
- PIs must follow the GDPR instructions from the Pre-Award team during the application/proposal development/submission process.
- PIs must follow GDPR instructions from the relevant contracting office during negotiation of a research contract or data use/material transfer agreement.

Recap – continued

- Once a contract or other research agreement has been fully executed, when conducting the research, the PI is required to meet all institutional and contractual GDPR requirements with respect to notification, consent, information security and privacy, and data acquisition, use, storage or sharing. This may require changes to lab/research group work flows, processes, record keeping, etc., to meet GDPR requirements.
- Known or suspected breaches of data subject to GDPR must be reported immediately by the PI to the hospital's Privacy Office for investigation by the Privacy Office/Information Security and institutional reporting, if necessary.

Where To Go for Help

- Submit general GDPR questions to the Partners Information Security Mailbox CISPO@partners.org. Questions will be reviewed daily and sent to the appropriate Partners or hospital office for response.
- For the most up-to-date GDPR information, including samples and templates, go to the Research Compliance page of the *Navigator*, <https://partnershealthcare.sharepoint.com/sites/phrmResources/c/Pages/GDPR.aspx>
- Continue to submit all applications, proposals, agreements, or IRB protocols that involve EU collaborators or sponsors through the appropriate Insight module.
- Report suspected and known breaches to the hospital privacy office, https://pulse.partners.org/resources_training/wikis/is/is_wiki_item/privacy_contacts_by_institution
- Hospital Information Security Officers are also available to help, https://pulse.partners.org/resources_training/wikis/is/is_wiki_item/security_contacts_by_institution

Acknowledgements

We would like to acknowledge the contributions of
Verrill Dana, LLP to this slide deck.