PREPARING FOR THE EU GDPR
IN RESEARCH SETTINGS

May 22, 2018[1]

[1] This guidance document is based on information available as of May 22, 2018. As the GDPR is enforced and further guidance is provided this document may need to be updated. Please contact the Johns Hopkins Legal Department to further analyze any effort you believe may implicate the GDPR.

Table of Contents

I. General Overview of the GDPR

WHAT IS THE GDPR?

The General Data Protection Regulation (GDPR) standardizes data protection law across all 28 European Union (EU) countries and imposes strict new rules on controlling and processing of personal information. It will come into effect as of May 25, 2018.

WHAT COUNTRIES ARE PART OF THE EU?

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

* Although not part of the EU, these countries will adopt the GDPR under the European Economic Area Agreement

WHAT ACTIVITIES DOES THE GDPR APPLY TO?

The GDPR applies to the "processing" of personal information by an individual or legal entity. The term "process" is extremely broad and generally covers anything that is done to or with personal data, whether by automated or manual means. This may include collecting, recording, organizing, structuring, storing, adapting, altering, retrieving, consulting, using, disclosing by transmission, disseminating or making available, aligning or combining, restricting, erasing, or destroying data.

CAN THE GDPR BE APPLIED TO COMPANIES LOCATED OUTSIDE THE EU?

Yes. GDPR applies to any organization that operates within the EU and processes personal information. The GDPR also applies to any organization outside of the EU that processes the personal information of an individual who is physically located in the EU which either (i) offers goods or services to such individual, or (ii) monitors the behavior of such individual. The GDPR does not cover individuals by virtue of their citizenship, but their physical presence in an EU country. For example, personal

information of an EU citizen collected at a U.S. location is not covered by the GDPR unless the controller or processor continue to monitor the EU citizen upon their return to the EU.

There are two different types of data-handlers the legislation applies to: "controllers" and "processors." A controller is an entity or person that "determines the purposes and means of processing of personal data" (e.g., as a sponsor, lead investigator, or primary research site). A processor is an entity or person that "processes personal data on behalf of the controller" (e.g., as a subcontractor, data coordinating center, or another study site). A processor may not by itself be subject to the GDPR except and until it has been engaged to provide data processing services to a controller. The controller will impose certain obligations related to data use and security on the processor through a written agreement. In addition, special rules apply to transfers of personal information out of the EU.

DOES PERSONAL INFORMATION INCLUDE MORE THAN JUST HEALTH RECORDS?

Yes. Although there are similarities between HIPAA and the GDPR, the GDPR is broader and covers information not covered by HIPAA. The GDPR applies to any information relating to an identified or identifiable natural person ("personal information"). Additional protections are given to "special categories" of or "sensitive" personal information." This includes information related to an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, processing of genetic data (including from an analysis of a biological sample), biometric data for the purpose of uniquely identifying a natural person (e.g., facial images or fingerprints), data concerning health (physical or mental), and data concerning a natural person's sex life or sexual orientation. In general, processing of health, genetic, and biometric data is prohibited unless the data subject has provided explicit consent or made the information publicly available or the processing is otherwise permitted by law.

WHAT IF THE INFORMATION IS DE-IDENTIFIED?

Unlike HIPAA, the GDPR does not provide specific methods to "de-identify" data. Rather, the regulation provides that data may be "anonymized" or "pseudonymized."

Anonymization of personal data refers to a subcategory of de-identification whereby direct and indirect personal identifiers have been removed and technical safeguards have been implemented such that data can never be re-identified (e.g., there is zero re-identification risk). The GDPR does not apply to data that does not relate to an identified or identifiable natural person or to data rendered anonymous in such a way that the data subject is not or no longer identifiable. A data set that is "de-identified" under HIPAA is not necessarily anonymized under the GDPR.

The GDPR defines pseudonymization as "the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person." Therefore, under the GDPR, pseudonymous data refers to data from which identifiers in a set of information are replaced with artificial identifiers, or pseudonyms, that are held separately and subject to technical safeguards. Unlike HIPAA, coded data must be treated as identifiable personal data and the GDPR does apply. Although pseudonymous data is not exempt from the GDPR altogether, the GDPR relaxes several requirements on controllers that use the technique such as allowing for additional use beyond the original

collection purpose. Pseudonymization may also allow for the controller to meet certain security requirements of the GDPR.

HOW CAN PERSONAL INFORMATION BE USED?	
Organizations governed by GDPR that collect or use personal information, including special category or sensitive information, may process such information only in certain circumstances. The regulation provides a number of mechanisms under which a GDPR covered entity may process personal information, including with the individual's express consent, for public health and scientific research, or in the provision of medical treatment (each, a "lawful basis").	
Consent	Data can be used in scientific research with the freely given, specific, informed, unambiguous, express written consent of the individual data subject. The consent documentation must include a "well-described purpose" for the scientific research and must be clearly distinguishable from other matters. Unfortunately, although the GDPR does recognize that it is often not possible to fully identify the purpose of data processing for research purposes at the time the data is collected, the consent cannot be broadly drafted. Guidance suggests that while the initial consent may be broad in nature, the data subjects would then be given the opportunity to consent to each individual use of the collected data as the new purpose becomes clear.
What if consent is withdrawn?	Under the GDPR, individuals have the "right to be forgotten" or "right of erasure." This means that upon the withdrawal of consent at any time, the controller should delete or anonymize the personal data straight away and its use of the data for the research study should stop. However, if the data needs to be retained after consent is withdrawn, the informed consent form must specify as such and indicate at the outset that, even if consent is withdrawn, the entity will retain the data for another identified lawful basis. However, this does not mean that the controller can swap from consent to another lawful basis. When data is processed for multiple purposes, the controller must be clear at the outset about which purpose applies to each element of data and which lawful basis is being relied upon.
Scientific Research Purpose – No Consent Needed	GDPR permits processing of special categories of personal information for scientific or historical research purposes. Under this mechanism, use must be limited such that it is proportionate to the aim pursued, respects the essence of the fundamental right to data protection, and provides for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. This implies that where the research purposes can be fulfilled by further processing which does not require the identification of data subjects then the research shall be fulfilled in a manner that does not permit such identification.

Public Health Purpose – No Consent Need	GDPR further permits the use of special categories of personal information on the basis of necessity 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. This basis for processing most directly authorizes health professionals to use special categories of personal data to protect public health in epidemics, pandemics, or other imminent safety threats in connection with drugs or devices. Hopkins should only rely on this basis to process personal data if the applicable research effort has a direct, immediate, non-attenuated public health application, but this basis may permit the processing of data concerning adverse events that arise in connection with the use of a drug or medical device.

DOES ANY INFORMATION NEED TO BE PROVIDED TO THE SUBJECT?

Yes. A controller must provide the data subject with a notice of the controller's privacy practices. This notice must be: (i) concise, transparent, intelligible, and easily accessible; (ii) written in clear and plain language, particularly if addressed to a child; and (iii) free of charge. Generally, the notice must answer the who/what/why/where/when/how questions related to data collection and use:

- What information is being collected/processed?
- Who is collecting/processing it (including contact information)?
- How is it collected/processed?
- Why is it being collected/processed, including the lawful basis?
- How will it be used?
- How will it be stored and for how long?
- Who will it be shared with (including third-parties)?
- What will be the effect of this on the individuals concerned?
- Is the intended use likely to cause individuals to object or complain?
- Will it be transferred to a third country and, if so, what is the lawful basis for such transfer?
- The data subjects must also be informed of their rights to request access, rectification, erasure or restriction of processing, to object to processing, and the right to data portability.

In the context of consented research, such notice can be built into the informed consent form.

WHAT ARE OUR DUTIES IF THERE IS A BREACH?

In the case of a personal data breach, data controllers shall without undue delay notify the appropriate regulator of the breach. The regulation goes on to state that, where feasible, this notification should take place no later than 72 hours after the breached party has become aware of the incident.

Further, if it is determined that the breach is likely to result in a high risk to an individual's rights and freedoms, such individual must also be notified of the breach. Internally, the research leaders should immediately contact the Johns Hopkins legal department.

WHAT ARE THE POSSIBLE PENALTIES IF WE FAIL TO COMPLY?

Fines are administered by individual member state supervisory authorities and vary depending on the type and scope of violation. There are two tiers of administrative fines that can be levied:

- Up to €10 million, or 2% annual global turnover – whichever is higher.
- Up to €20 million, or 4% annual global turnover – whichever is higher.

The fines are based on the specific articles of the Regulation that the organization has breached, taking into account certain aggravating and mitigating circumstances. Infringements of the organization's obligations, including data security breaches, will be subject to the lower level, whereas infringements of an individual's privacy rights will be subject to the higher level.

II. HIPAA v. GDPR

GEOGRAPHIC SCOPE	
HIPAA	**GDPR**
Limited to organizations that meet the definition of a "Covered Entity" or a "Business Associate" HIPAA does not address extraterritoriality	The GDPR also applies to any organization outside of the EU that processes the personal information of an individual who is physically located in the EU which either (i) offers goods or services to such individual, or (ii) monitors the behavior of such individual

ROLES IN DATA COLLECTION AND USE	
HIPAA	**GDPR**
"Covered Entity" – health plans, health care clearinghouses, and health care providers who electronically transmit health information for certain transactions "Business Associate" - performs or assists in performing, for or on behalf of a covered entity, a function or activity regulated by HIPAA	"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 "Processor" - a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

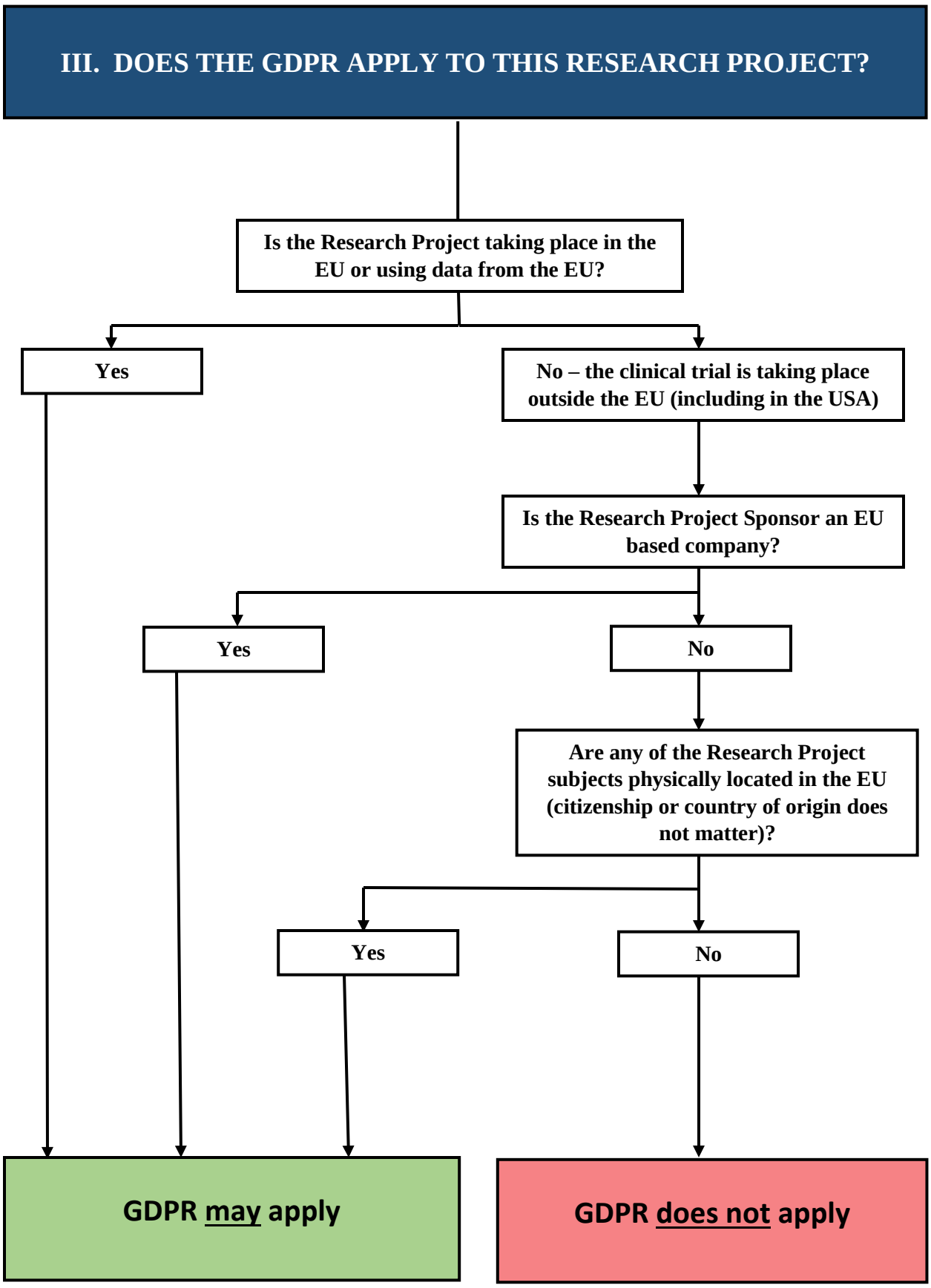
COVERED DATA	
HIPAA	**GDPR**
"PHI" – individually identifiable health information created or received by a health care provider, health plan, or health care clearinghouse	"Personal Data" - any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This would include data on the PI or research team members. "Special Category Data" - race; ethnic origin; politics (including opinions); religion; trade union membership; genetics; biometrics (where used for ID purposes); health; sex life; or sexual orientation. "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 his or her health status

DE-IDENTIFIED DATA	
HIPAA	**GDPR**
"De-Identified Data" - Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information 18 identifiers must be removed Once properly de-identified then no longer considered PHI and subject to HIPAA	"Anonymized Data" - data rendered irreversibly anonymous in such a way that the data subject is not or no longer identifiable "Pseudonymization" - the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information.

TRANSPARENCY	
HIPAA	**GDPR**
Notice of Privacy Practices - provides a clear, user friendly explanation of individuals' rights with respect to their personal health information and the privacy practices of health plans and health care providers.	Privacy Policy – notice to individuals must be: • concise, transparent, intelligible and easily accessible; • written in clear and plain language, particularly if addressed to a child; and • free of charge.

PROCESSING AND USE OF DATA	
HIPAA	**GDPR**
"Use" - the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information "Disclosure" - the release, transfer, provision of, access to, or divulging in any other manner, of information outside the entity holding the information	"Processing" - any operation or set of operations which is performed on personal data or on sets of personal data Includes collection and storage – impossible to come into contact with data without being considered to be "processing" that data

PERMITTED PROCESSING AND USE		
	HIPAA	**GDPR**
Consent	Permitted pursuant to an individual's authorization, which must include a number of required elements.	Permitted if the data subject has freely given consent to the processing of his or her personal data for one or more specific purposes
Medical Treatment	"Treatment" exception is part of the standard "TPO Exception" (treatment, payment, operations)	Permitted when necessary for the purposes of medical diagnosis, the provision treatment or management of health systems.
Legally Required	Permitted when disclosure is required by law	Permitted to comply with a legal obligation
General	PHI may be used or disclosed for the administration of the entity holding the data or to fulfill its obligations under a contract	Permitted when processing is necessary for the purposes of the legitimate interests pursued by the controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject
Research	PHI may be disclosed for research purposes – limited data set with DUA, consent, IRB waiver	Permitted for scientific and historical research purposes or statistical purposes – must have safeguards in place


III. DOES THE GDPR APPLY TO THIS RESEARCH PROJECT?
Is the Research Project taking place in the EU or using data from the EU?
Yes
No – the clinical trial is taking place outside the EU (including in the USA)
Is the Research Project Sponsor an EU based company?
Yes
No
Are any of the Research Project subjects physically located in the EU (citizenship or country of origin does not matter)?
Yes
No
GDPR may apply
GDPR does not apply

IV. WHAT TO EXPECT IF THE GDPR APPLIES

WILL JOHNS HOPKINS BE A CONTROLLER OR PROCESSOR?

Johns Hopkins' role will depend on various factors and should be analyzed on a case-by-case basis.

WHAT ARE JOHNS HOPKINS' RESPONSIBILITIES AS A CONTROLLER?

To the extent the GDPR applies and Johns Hopkins is the controller, Johns Hopkins will be primarily responsible for compliance with the GDPR. This means that Johns Hopkins would need to make the initial determination as to what lawful basis personal information will be collected and processed under – consent, scientific research, or public health. This decision will likely need to be made on a case-by-case basis and take into account the pros and cons of each approach.

Johns Hopkins will also be responsible for drafting those documents that will be delivered to the individual research subject(s) and the agreements that will need to be put in place with any subcontractors or other parties who are operating as processors.

WHAT IS A DESIGNATED PRIVACY OFFICER AND WOULD WE NEED ONE?

Under the GDPR a controller must have a Designated Privacy Officer (DPO) in certain circumstances. DPOs monitor internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs), and act as a contact point for data subjects and the supervisory authority. The DPO must be independent, an expert in data protection, adequately resourced, and report to the highest management level.

A DPO is required in the event one or both of the following statements is true:

1) An entity's core activities consist of processing personal information which requires regular and systemic monitoring of individuals on a large scale; or

2) An entity's core activities consist of processing personal information which is about special categories on a large scale or about criminal convictions and offences.

An initial determination has been made that in the context of research, Johns Hopkins is not required to appoint a DPO.

WHAT ARE JOHNS HOPKINS' RESPONSIBILITIES AS A PROCESSOR?

If Johns Hopkins serves as a processor, the controller (which will likely be the sponsor) will pass on certain obligations and responsibilities related to GDPR compliance through a written agreement. This may include certain required model clauses, data security standards, and drafts of the documents that must be provided to the research subjects (e.g., consents, privacy policies, etc.). The legal department should be consulted if this situation occurs.

To the extent the GDPR does not apply but the sponsor does not agree and requests additional language to be included in applicable agreements or requests additional documents be provided to research subjects, language such as the following can be added: "Johns Hopkins shall comply with the provisions of the GDPR ***to the extent applicable.***" Consult with the legal department for any further requests.

V. SAMPLE SCENARIOS AND APPLICATION OF GDPR

SCENARIO 1: Johns Hopkins Hospital (JHH) is a site under a trial awarded to an EU institution.	
Facts	JHH is serving as a site in a study **solely** developed and awarded by an industry sponsor to an EU institution. JHH, operating under a subcontract from the EU institution, will be sending U.S. subject data to the EU. No EU data will be coming to the U.S.
Analysis	JHH is not providing goods or services to or monitoring the behavior of subjects in the EU, thus **it is not directly subject to the GDPR.** Additionally, JHH is not processing EU subject data on behalf of the EU entity, so it is not a processor. If JHH subject data will be sent to the EU, the EU institution may ask JHH to revise its consent forms and/or provide a notice to subjects to comply with the GDPR so the EU institution's processing of that data in the EU is permitted under the GDPR.

SCENARIO 2: Johns Hopkins University School of Medicine (JHUSOM) has received a grant and is collaborating with EU entities.	
Facts	JHUSOM has a received a grant to conduct a study that includes sites in Germany (working under subcontracts from JHUSOM) collecting data on subjects located in Germany. Subject data will be sent from the EU to the U.S. for analysis as part of the study.
Analysis	By receiving and analyzing data from the German site, JHUSOM is monitoring the behavior of (and potentially indirectly providing research-related services to) data subjects in the EU as the "sponsor" of the study. Thus, **GDPR applies to JHUSOM as a controller.**

SCENARIO 3: Johns Hopkins University School of Public Health (JHUSPH) is serving as a Data Coordinating Center (DCC) for a trial.	
Facts	JHUSOPH is serving as the DCC for a multi-national study that includes sites in the EU and is receiving coded and/or HIPAA de-identified data from all sites, including those in the EU.
Analysis	**JHUSPH is a processor** because as the DCC, JHUSOPH is processing personal data of EU subjects on behalf of the sponsor. A written agreement between the sponsor and JHUSOPH (and any third-parties) will provide the obligations and responsibilities of JHUSOPH related to data use and analysis. The personal data JHUSPH processes includes both (i) coded personal data of EU study participants, and (ii) fully identifiable data of EU investigators and study staff. **De-identified data is still subject to GDPR if a key exists to "re-identify" the data.**

SCENARIO 4: JHUSOM is a trial site for a sponsored clinical trial with EU sites related to human tissue analysis.	
Facts	JHUSOM pathologist has been engaged to perform skin biopsy reads on human tissue samples collected by a sponsor conducting a study at multiple EU sites. The pathologist receives coded and/or HIPAA de-identified biopsy samples to provide reads and feedback reports. At the conclusion of the study, JHUSOM is permitted to keep samples for own secondary research purposes.
Analysis	**GDPR will apply to both the original use and analysis of the data and the secondary use.** JHUSOM is a processor for the initial use because JHUSOM is processing tissue samples that can be re-identified on behalf of the sponsor. A written agreement between the sponsor and JHUSOM will provide the obligations and responsibilities of JHUSOPH related to data use and analysis. For any secondary use, JHUSOM will become the controller and will need to obtain express consent from the study subjects for the secondary use or rely on another lawful basis (scientific research or public health). Under GDPR, bio-specimens cannot be anonymized and remain subject to GDPR even if de-identified for the purposes of HIPAA.

SCENARIO 5: JHUSOM performs a clinical trial that requires continued monitoring of trial participants when they return home to the EU.	
Facts	JHUSOM is conducting a clinical trial which requires trial participants to be physically present at the Hopkins site during the initial steps of the trial. Upon the completion of such initial steps, the participants may return home by JHUSOM will continue to monitor certain data points for a certain duration of time. One participant resides in Spain and will return to Spain after the initial steps of the trial.
Analysis	**GDPR will apply to the study as JHUSOM is monitoring the behavior of an EU resident.** JHUSOM is a controller under the GDPR because it controls the data. The consent documents signed by the EU resident participant will include language that specifically addresses the continued monitoring of his/her behavior and health after returning to the EU. This is a lawful basis under which the personal data can be processed.