Guidance for General Data Protection Regulations (GDPR) compliance in the conduct of human research.

Note: GDPR is a much larger issue that reaches far beyond the conduct of research. The following is provided by the NU IRB as guidance for researchers as to what the compliance expectations are based on reading the GDPR regulations and discussing the application with our colleagues in other countries.

However, to date there is no published guidance documents associated with the GDPR and every country has their own interpretation so there are some facets of implementation of GDPR compliance of which we are not entirely sure. This document will be updated as more information is provided.

Feel free to contact the NU IRB office if you have any questions. However, if you are collaborating with another researcher in a country that has signed on to the GDPR, a more directly reliable resource for what it required in that country may be the local IRB, EC or RRB.

I. Quick Q and A for GDPR and the conduct of human research:

Q-1: Who needs to pay attention to GDPR compliance? (For more information see: Sec_A Sec_B below.)

A-1.1: Anyone doing research that involves research activity that is collecting information or data in person or online from anyone (known as a "data subject") who is in one of the countries of the European Economic Area. This affects people living or traveling in a GDPR complaint country and is unrelated to citizenship.

A-1.2: The countries are: Austria, Belgium, Bulgaria, Czech Republic, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and the United Kingdom. In addition there are other countries that are also GDPR compliant by their own regulations.

In addition to the countries of the EEA which have signed onto the GDPR, there are a number of other countries deemed to have sufficient data protection such that EU data can be transferred there without additional protections. These countries are: Andorra, Argentina, Canada, the Faroe Islands, Guernsey, Israel, the Isle of Man, Jersey, New Zealand, Switzerland, and Uruguay. The U.S. is not considered to have adequate data protections and so full compliance with GDPR is expected prior to the collection and transfer of data.

Q-2: What is the most likely impact on my research?

A-2.1: The consent process will be a two-step process that includes a Letter of Information and a Consent Document. (See Sec_G below and HRP-590 GDPR written_consent_form_template)

A-2.2: Enhanced data protection. (See HRP-335 GDPR Data Protection Worksheet)

Q-3: What about anonymous data or use of deidentified data? (see Sec_H)

A-3: Anonymous data are not subject to GDPR. Deidentified data also are not subject to GDPR provided the research team had no role in the collection of the data with identifiers in the first place and has no access to the identifiers going forward. A data use agreement may be applicable.

Q-4: What constitutes identifiable personal data under GDPR? (see Sec_C1)

A-4: "Personal data" is all information which is related to an identified or identifiable natural person. Those impacted are identifiable if they can be identified, especially using assignment to an identifier such as a name, an identifying number, location data, an online identifier or one of several special characteristics, which expresses the physical, physiological, genetic, mental, commercial, cultural or social identity of these natural persons. In practice, these also include all data which are or can be assigned to a person in any kind of way. For example, the telephone number, credit card or personnel number of a person, account data, number plate, appearance and customer number of address are all personal data.

Since the definition includes "all information," you must assume that the term "personal data" should be as broadly interpreted as possible. These include also less-clear information, such as political opinions, sexual orientation, and religious affiliation. Even such mundane data items such as recordings of work times which include information about the time when an employee begins and ends his work day, or written answers from a test-taker and any remarks from the test about these answers are "personal data" if the test-taker can be theoretically identified.

All of which is by way of saying: the definition of identifiable under GDPR is far more extensive than what we traditionally interpret as identifiable in the U.S. If you are collecting the data yourself from people in a GDPR compliant country assume that you need to take a very conservative perspective of data collection, data management and data protection.

Q-5: What are the rights of data subjects that I need to consider under GDPR? (see #Sec_F)

A-5: Most are the same or similar to the rights of research participants under Belmont and the Federal Regulations. The two that are different are the Right to Erasure/Right to be Forgotten and the Right to Reject Automatic Profiling. The right to be forgotten means the right to complete removal of the person and their data from the study at their request, even well after the fact. There is no guidance on what this means in terms of de-identification if the EEA participant has the right at any time to remove their data from a data set.

Similarly, the right to reject profiling may have implications with regard to algorithms used to determine eligibility and so forth. There is no guidance on this either so we do not know what the impact of this right will be going forward.

Q-6: What if we are relying on another IRB to be the IRB of record, who is responsible for GDPR compliance?

A-6: Technically the IRB of record, whether another institution or a commercial IRB, should set the standard for what is needed to be GDPR compliant. However, everyone should be mindful of GDPR and should raise questions if the NU site is collecting; receiving; or managing data in any way that is affected by GDPR.

Q-6: What are the consequences of non-compliance? See Sec_E

A-6 Verbal reprimand for minor offenses and more typically fines.

II. The Details:

A. What is GDPR:

GDPR, or Regulation (EU) 2016/6793 of the European Parliament and of the Council, is an EU legislation that protects natural persons with regard to the processing of personal data and on the free movement of such data. The GDPR replaces the EU Data Protection Directive and is designed to update and harmonize data privacy laws across the countries of the European Economic Area (EEA), which includes the 27 countries for the EU plus three countries (Norway, Iceland and Liechtenstein). Countries that belong to the EEA include Austria, Belgium, Bulgaria, Czech Republic, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, United Kingdom.

The GDPR is designed to protect the privacy of individuals in the EEA and to reshape the way organizations with operations or customers in the EU approach data privacy and data portability.

As such, the GDPR:

1. Establishes the circumstances under which it is lawful to collect, use, disclose, destroy or otherwise "process" Personal Data, including when conducting clinical research activities;

2. Establishes certain rights of individuals in the EEA, including rights to access, amendment and erasure (referred to as the right to be forgotten);

3. Requires Personal Data controllers and processors to implement appropriate technical and organizational security measures to ensure a level of data security that is appropriate to the risk to Personal Data; and

4. Requires notification to data protection authorities and affected individuals following the discovery of a "personal data breach," which is breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

B. Who is protected by GDPR:

All "data subjects" who are in any EEA country for any reason. The application of GDPR is unrelated to citizenship. For example: U.S. citizens traveling to Spain could be 'data subjects' and would be protected by GDPR.

C. Definitions:

1. Personal Data: (https://gdpr-info.eu/issues/personal-data/):

   The term 'personal data' is the entryway to application of the Data Protection Basic Regulation and is defined in Art. 4 para. 1 no.1. Personal data are all information which is related to an identified or identifiable natural person.

   Those impacted are identifiable if they can be identified, especially using assignment to an identifier such as a name, an identifying number, location data, an online identifier or one of several special characteristics, which expresses the physical, physiological, genetic, mental, commercial, cultural or social identity of these natural persons. In practice, these also include all data which are or can be assigned to a person in any kind of way. For example, the telephone number, credit card or personnel number of a person, account data, number plate, appearance and customer number of address are all personal data.

   Since the definition includes "all information," one must assume that the term "personal data" should be as broadly interpreted as possible. This is also found in case law of the European Court. These include also less-clear information, such as recordings of work times which include information about the time when an employee begins and ends his work day, as well as breaks or times which do not fall in work time. Also, written answers from a test-taker and any remarks from the test about these answers are "personal data" if the test-taker can be theoretically identified. The same also applies to IP addresses. If the processor has the legal option to oblige the provider to publish additional information which can identify the user who is behind the IP address, this is also personal data. In addition, one must note that personal data need not be objective. Subjective information such as opinions, judgements or estimates can be personal data. Thus, this includes an assessment of creditworthiness of a person or an estimate of work performance by an employer.

   Last but not least, the law states that the information for a personnel reference must refer to a natural person. In other words, data protection does not apply to information about legal entities such as corporations, foundations and institutions. For natural persons, on the other hand, protection begins and is extinguished with legal capacity. A person obtains this capacity with his birth, and loses it upon his death. Data must therefore be assignable to specific or specifiable living persons for reference to a person.

   Data is not "Personal Data" merely because it concerns a citizen of an EEA country. Instead, the data must concern an individual located in an EEA single market country unrelated to whether that person is a citizen or not of that country. There is agreement that individually identifiable data collected from an EEA citizen at a location in the United States will be subject to United States law and not GDPR. However, if the

organization or the researcher continues to monitor the person citizen after returning to the EEA then GDPR does apply.

2. 'Controller' means 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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law. For example, a sponsor of a research study would typically be a "controller."

3. 'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. For example, the PI of a sponsored research study would typically be a "processor." For a self-initiated study the PI would be the controller and the processor.

4. 'Recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

5. 'Consent' of the data subject means 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 relating to him or her (see additional information below regarding "rights".)

6. 'Personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

7. 'Genetic data' means 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 natural person in question.

8. 'Biometric data' means 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 (finger print) data.

9. 'Data concerning health' means 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.

D. <u>What is the reach of GDPR</u>:

The GDPR applies to research located within the EEA and to research located outside of the EEA if they offer "goods or services" to, or monitor the behavior of EEA data subjects within the

EEA. It applies to all collecting, processing and holding the personal data of data subjects residing in the EEA and is unrelated to where the company (or researcher) resides. The GDPR has direct reach to a controller or processor organization located in the United States or otherwise outside the EEA if the organization:

1. Creates an establishment in the EEA;

2. Offers "goods or services" (even if free) to individuals in the EEA, such as by advertising in the EU. The "offering of goods or services" is more than mere access to a website or email address, but the purposes of considering "goods and services" as it relates to research, some research may meet the definition of "offering goods and services" and some may not. Depending on the study, "goods and services" may be as simple as the 'opportunity to participate' in a research unrelated to compensation though compensation is typically viewed as "offering goods and services."

3. Monitors the behavior of individuals in the EEA, such as by continuing to monitor patients after they return to the EEA as part of, for example, post-discharge care. The monitoring of behavior will occur, for example, where individuals are tracked on the internet by techniques that apply a profile to enable decisions to be made/predict personal preferences, etc. This means in practice research outside the EEA that is targeting consumers or participants in the EEA will be subject to the GDPR.

E. Penalties for non-compliance:

According to Article 83, depending on the nature of the infringement and the cooperation with a remedy, fines are the primary method of dealing with non-compliance with the specific guidance being: "Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher."

F. Data Subject's Rights under GDPR:

GDPR strengthens and defines the individual rights to be considered in systems, organizational privacy policies and explicit consent. In the absence of clarifying guidance, all of the rights under GDPR are listed below although not all may apply to research in the same way that they may apply to organizational systems. The rights include:

1. Right of Access: Data Subject Access Requests (DSAR) – e.g. "What do you know about me?"

2. Right to Erasure/Right to be Forgotten – e.g. "Remove me from your database"

3. Right to Rectification which is the right "Amend or correct my details." This is a "data subject's" right under GDPR but it is not clear this would apply to research although it could easily be interpreted to apply to research subject pools or registries.

4. Right to Restrict Data Processing – e.g. "Stop filming me"

5. Right to Withdrawal of Consent – "I don't want to do this survey anymore"

6. Right of Data Portability – e.g. "'Move my personal data from one location to another location. (This is a data subject's right under GDPR but it is not clear this would apply to research.)

7. Strengthened right to prior notification before data collection

8. Right to Reject Automated Profiling: This is a new concept under the GDPR. Profiling is automated processing that is used to evaluate personal aspects of an individual, e.g. being refused insurance based on automated algorithm. It is not known at this time if this would impact automatic profiling for eligibility / screening for a study or even the emerging research that is designed specifically to improve methods of profiling as it relates to health risks or even consumer behavior.

G. Consent requirements under GDPR:

1. GDPR permits researchers to rely upon consent from research subjects as a lawful basis for processing Personal Data for research purposes typically under 'public interest' as the most appropriate legal basis. To obtain a valid consent to processing an individual's Personal Data for research purposes under GDPR, the individual's consent must be:

    a. **Freely given**: The individual must have a realistic choice, or the realistic ability to refuse or withdraw consent without detriment. Similar to US law, coerced consents are not compliant with GDPR.

    b. **Specific**: The consent must include a specific, transparent statement of each purpose of the study and including the rights articulated above. This includes specific reference for "future use" of the data.

    c. **Informed**: An individual must be informed of the nature and extent to which the individual is consenting to what data collection activities and to what use of data.

    d. **Unambiguous**: GDPR requires a statement or "clear affirmative act" that indicates the individual has agreed to the proposed processing of data activities. Silence, pre-checked boxes and inactivity (passive consent) are not allowed for the purposes of consent.

2. The consent process needs to be a distinct two-step process that includes a Letter of Information as one document and a Consent Document as a separate document.

    a. Letter of Information: This is essentially the same as the consent document that we currently use but with the optional elements and the signatures removed to a separate sheet. Use whatever protocol template is appropriate for your study and complete the information as you usually would except refer to HRP-335 GDPR Data Protection for additional information in adding specific detail to your data management and data protections sections of the study. This is the part of the consent process is a separate step in support of "freely given." All of the same elements that are in the NU current consent templates are required and at the end there needs to be the contact information so the potential participant who has questions, knows who to contact.

b. Consent Document (see HRP-590): This document will be a page or two and include all of the specific elements of the study that the potential participant has read through in the Letter of Information. On the Consent Document the individual will specifically agree to each element by initialing in the box. The consent document should be transparent, specific, and unambiguous with each sentence. The signatures will be as they currently are the NU IRB consent template.

c. Note: It does not appear that waiver of consent or waiver of documentation is acceptable under GDPR with the exception of exempt projects where a check box with "I agree" could serve as sufficient proactive affirmation of consent. Different countries will have different guidelines. When in doubt, it is recommended that you use a test box where the participant can type in their name as an 'electronic signature' however, it is important to know that it is possible that will not be acceptable.

H. What about anonymous data? Can personal data be de-identified for future use?

Recital 26 is clear: "The principles of data protection should apply to any information concerning an identified or identifiable natural person….The principles of data protection should therefore not apply to anonymous information, namely 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. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes."

That said, the same Recital references further the issue of personal data which have undergone "pseudonymization" which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. The focus is on the possibility of reidentification either by the controller or by another person to identify the natural person directly or indirectly. Generally, EEA data protection authorities deem data to be de-identified if there is no reasonable means through which someone who has access to the data could use the data to re-identify an individual who is the subject of the data. It seems as though de-identification under GDPR would be similar to de-identification under HIPAA or any sensitive data set: for example: for key-coded data to be de-identified the holder of the data must not have access to the re-identification key or possess any other means to re-identify the individuals who are the subjects of the data. This is not different from what is usual practice in the United States except that the definition of identifiers is more broadly defined.

Resources:

Barnes, M.; et al. (2018): New Draft guidelines on GDPR consent requirement's application to scientific research. (https://biglawbusiness.com/new-draft-guidelines-on-gdpr-consent-requirements-application-to-scientific-research/).

Broccolo, B. M.; et al. (2018): Does GDPR Regulate My Research Studies in the United States? (https://www.mwe.com/en/thought-leadership/publications/2018/02/does-gdpr-regulate-research-studies-united-states).

GDPR interactive searchable version online: (https://gdpr-info.eu/).

GDPR pdf English version of regulation: http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf

"Guidelines on consent under Regulation 2016/679": https://www.mayerbrown.com/files/uploads/Documents//PDFs//2017//December//wp259_enpdf__2_.pdf

Mayer Brown Legal Update] (12-2017): New draft consent guidelines under the GDPR: What You Need to Know. https://www.mayerbrown.com/publications/detailprint.aspx?publication=14187

Santos, J. (12-2017): Healthcare researchers prepare for GDPR: what does GDPR mean for health care researchers? Kantar Health (http://www.kantarhealth.com/docs/white-papers/healthcare-researchers-prepare-for-gdpr.pdf?sfvrsn=10).