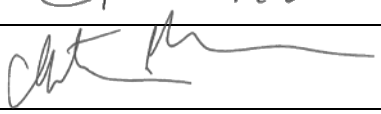
OFFICE OF THE INSTITUTIONAL REVIEW BOARD

Standard Operating Procedures		
SOP #513.0 Revision 0	**TITLE: Compliance with the European Union's General Data Protection Regulation (GDPR)**	Effective Date: 5/25/2018
Approved By: OIRB Director	Signature 	Date 5/25/2018
Approved By: IRB Chair	Signature 	Date 5/25/2018

PURPOSE
To describe human research requirements to maintain compliance with the European Union's (EU) GDPR.

REVISIONS FROM PREVIOUS VERSION
None

POLICY
The GDPR is a broad-scale regulation designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens' data privacy and to reshape the way organizations across the region approach data privacy. The GDPR applies to *all personal data* collected in EU and non-EU European Economic Area (EEA) countries.

EU countries include Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the UK. The EEA includes EU countries and also Iceland, Liechtenstein and Norway.

The GDPR applies to **US-based organizations** if the organization: 1) offers goods or services (including research services) to individuals in the EEA, 2) is established in the EEA and acts as a data controller or processor, and/or 3) monitors the behavior of individuals in the EEA (e.g. multi-site research in EEA, mobile application research).

UNM human researchers must comply with the provisions of the GDPR when they:

- Target and/or recruit participants who reside in EEA countries (including online research), and/or
- Conduct research in or collect data from countries covered by the GDPR.

DEFINITIONS
Anonymized data is data in which there are no identifiable persons, i.e. all personal identifiers have been removed.

Controller is one who alone or jointly with others determines the purposes and means of processing personal data (such as the Principal Investigator of a study). Controllers have many responsibilities including providing notices to data subjects, responding to exercise of subject rights, appointing

representative in EEA, notifying supervisory authorities and data subjects of data breaches, and maintaining records of processing.

Identifiable person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person. Parental consent is required to process the personal data of children under the age of 16 for online services.

Legal basis is a GDPR-specific term that is a justification for the collection and processing of personal data. The legal basis options that would affect human research are:

- Consent **-** the individual has given clear consent for you to process their personal data for a specific purpose.
- Legitimate interests **-** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data that overrides those legitimate interests. The existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place (examples include performance of a contract, vital interest or public interest).

Personal data is any information relating to an *identifiable person***.** *Special categories of personal data* are defined in the GDPR as potentially sensitive data and include racial or ethnic origin, data concerning health, data concerning a natural person's sex life or sexual orientation, genetic data, biometric data used for the purpose of uniquely identifying an individual, and political opinions, religious or philosophical beliefs, or trade union membership. Personal data relating to criminal convictions and offenses are not included, but similar extra safeguards apply to its storage and use.

The processing of personal data for purposes other than those for which the personal data were initially collected is allowed only where the processing is compatible with the purposes for which the personal data were initially collected. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered compatible lawful processing operations.

Processor is one who processes personal data on behalf of the controller. Both controllers and processors are regulated directly under GDPR.

Pseudonymised data is coded data. It is considered to be *personal data* subject to the protections of the GDPR. This is in contrast to the Common Rule, which generally does not protect such information as "identifiable private information" provided that certain steps are taken to prevent the researcher from obtaining the means to link the code to the participant's identity.

A *Privacy Notice* is another GDPR-specific term that refers to the notification required for the collection and transfer of the data of *identifiable persons*. For IRB purposes, the Consent Form serves as the Privacy Notice. Requirements for a Privacy Notice are listed below.

PROCEDURE

1. GDPR requirements must be addressed in the IRB protocol and consent form. Considerations include:
    a. The period for which the data will be stored.
    b. Any projected future use of the data.
    c. Ability for data subject to be "forgotten" (data deleted or anonymized) upon request.
2. The following information must be included in the IRB protocol:
    a. Data Collection Procedures and Data Management Section
        i. Proposed uses and storage of the data, including any expected future use.
        ii. Statement that data will be deleted or anonymized immediately if a participant withdraws their consent or otherwise requests that they be "forgotten."
    b. Confidentiality Section
        i. The period for which the data will be stored, or the criteria used to determine that period.
        ii. Recipients of data if outside of identified project team.
3. The following information must be included in the Consent Form/Privacy Notice (see Additional Elements of Consent template):
    a. Contact details for data controller (researcher)
    b. Contact details for data protection office, if applicable
    c. Purpose of processing (project purpose and procedures) – Note: use of identifiable data beyond the original uses stated in the consent form will require re-consent of the participants.
    d. Recipients (or category of recipients) of data
    e. Source of data if not from participant
    f. Information about international data transfer and safeguards, if applicable
    g. Period of data storage or criteria for determining period of data storage
    h. Statement that data will be deleted or anonymized upon request or upon withdrawal of consent.

REFERENCES

GDPR Portal - https://www.eugdpr.org/
UK International Commissioner's Office - https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/