**Data Security: GDPR**

**What is GDPR?**

The General Data Protection Regulation (GDPR) is a new regulation affecting the European Economic Area (EEA), which includes all European Union (EU) countries and non-EU countries Iceland, Liechtenstein and Norway.  Effective May 25, 2018, the GDPR is designed to harmonize data privacy laws across Europe and imposes stringent data protection requirements on entities, including those based outside of the EU, that process “personal data” of individuals in the EEA.  It doesn’t apply to the processing of personal data of deceased persons or of legal entities.

* GDPR defines “personal data’’ broadly to include:
  + “**[A]ny information relating to an identified or identifiable natural person**(“data subject”).”
* “An identifiable person is one who can be identified, **directly or indirectly**, in particular 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.’’

**What does GDPR Require?**

GDPR grants a number of rights to people whose personal data is collected, stored, or “processed” by people or organizations, including:

* Right to be informed
* Right of access|
* Right to rectification
* Right to erasure
* Right to restriction of processing
* Right to data portability
* Right to object
* Rights regarding automated decision making

* Personal data is any information that relates to an identified or identifiable living individual.  **NOTE: data that has been “de-identified” under HIPAA may still qualify as “personal data” and be protected under the GDPR**.
* There are additional requirements for use of “Sensitive Personal Data” which is data that includes information related to: an individual’s racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic data; biometric information; health data; or sexual life or orientation.
* The term “processing” covers a wide range of operations performed on personal data. It includes the collection, recording, organizing, structuring, storage, adaptation or alteration, retrieval, use, disclosure, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data.

 In order to ensure those rights are upheld, users of personal data that is protected by the GDPRmay be required to do the following.

* Obtain consent of subjects for data processing.  NOTE: Consent requirements under the GDPR are more specific than informed consent requirements under U.S. law.
* Anonymize collected data to protect privacy.
* Provision of data breach notifications.
* Safely handle the transfer of data across borders.
* Certain organizations must appoint a data protection officer to oversee GDPR compliance.

Compliance with GDPR is overseen by Data Protection Authorities (DPA) in the EU member states.  DPAs have investigative and corrective powers related to the application of the data protection law.

**Does GDPR apply to Wake Forest University Health Sciences (WFUHS) research?**

It depends on the project.

* The GDPR applies to organizations located outside of the EU if they are offering goods/services (paid or for free) to EU citizens or monitoring the behavior of individuals in the EU.  If a research project will be conducted in the EU or recruitment of participants will be directed to people in the EU, then GDPR would apply for the data collected and stored in the EU.
* There must also be a basis to legitimize the transfer of data from the EU to a US organization, and the GDPR may require that EU participants be notified that their data will be sent to a location where it will not be protected by GDPR.
* Note that some sponsors or collaborators may include general statements in contractual agreements that would obligate WFUHS researchers to follow GDPR standards for the project even though the data will be located in the US.  The CTSI Office of Sponsored Programs must be notified when a research receives such contractual agreements and the Office will help in reviewing and negotiating those terms.

Notify IT Security, the Privacy Office, and the CTSI Office of Sponsored Programs as early as possible so that we can evaluate the specific needs for your study and work with any collaborators or sponsors on the most appropriate agreements.  Contact information is below.

**I am considering a project or contract which requires compliance with the GDPR. Where do I start?**

* Notify IT Security, the Privacy Office, and the CTSI Office of Sponsored Programs.   They will help with establishing a compliance plan.

**What are the benefits of being GDPR compliant?**

* It is important that we handle all data appropriately and respect the rights of research participants as required by the consent form, the Institutional Review Board requirements, contractual obligations, legal requirements, and WFBMC policies.  By doing this our investigators should continue to enjoy opportunities to conduct research and collaborate with colleagues in the EEA.

**What are the risks of non-compliance?**

* It is currently unclear what the specific consequences for failure to comply with GDPR will be.  The penalties will be set by individual states and must be “effective, proportionate, and dissuasive” according to the regulation.  It is safe to assume that the results of noncompliance will be very unpleasant and may include civil and/or other penalties.  In addition, failure to comply with the GDPR could expose the institution to reputational damage and loss of future research awards.

**How are GDPR requirements different from our general data security requirements?**

* Unclassified Information (*see FAQs on CUI*).  In addition, all Medical Center policies regarding data privacy and security should be followed.  IT Security can help develop the data storage and sharing plan for individual projects.

**How do I determine if the GDPR applies to my project?**

* You will need to evaluate whether your project involves the use of personal data regarding individuals residing in the EU, the geographic location of the study data collection, storage, processing or transfer, and/or specification in the contract or award notification.
* The CTSI Office of Sponsored Programs can help in evaluating whether the GDPR applies to your project.

**What are GDPR controls?**

The regulation requires implementation of appropriate technical and organizational measures which are designed to protect data from unauthorized access or disclosure; and that only the minimum quantity of personal data are processed for each authorized purpose.

**How will GDPR impact the use of my data?**

* It will depend on a multitude of factors, including the nature of the data being used, the nature of the research study (for example, is this prospective or secondary research), where the data resides, whether a study subject has exercised any rights he/she has under the GDPR, and other considerations.  If you have personal data regarding individuals who reside in the EU, please contact the CTSI Office of Sponsored Programs to request an evaluation of how the GDPR may impact the use of your data.

**What are we doing at the institutional level to comply with GDPR requirements?**

* A committee has been established with representatives from IT, CTSI, and other research stakeholders to address institutional needs related to GDPR.
* The Legal Department and senior leaders are working with IT Security, Privacy and CTSI Office of Sponsored Programs on all agreements involving GDPR.

**What resources are available to assist me/my team with GDPR related questions?**

* Consultation and assistance are available for reviewing grant proposals, contracts, and notices of award for GDPR requirements: contact CTSI Office of Sponsored Programs, Ryan Favreau at 336-713-5306.
* Consultation and assistance are also available for conducting risk assessments, and training for PIs and study teams. Contact IT Security at 336-713-ITSO (3-4876) or [ITsecurity\_dl@wakehealth.edu](mailto:ITsecurity_dl@wakehealth.edu) or [privacy@wakehealth.edu](mailto:privacy@wakehealth.edu) for assistance.

**Important Links**

European Commission: [2018 reform if EU data protection rules](https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en#abouttheregulationanddataprotection)