General Data Protection Regulation (GDPR) and Human Subjects Research

This guidance outlines some of the critical ways GDPR impacts the conduct of human subjects research involving the European Economic Area (EEA) and/or the United Kingdom*. Research involving the collection of personal data on individuals within the EEA, whether through in-person or electronic methods (e.g., online or email), requires compliance with GDPR.

GDPR creates onerous compliance challenges and significant financial risks for the University and our researchers. The main areas of impact are changes to the consent process, modified contractual language in research and vendor agreements, increased data protection and technical security requirements, and prompt breach notification requirements (72 hours).

Researchers should think carefully before choosing to involve a site in the EEA in their research. Researchers must consult with COMIRB, Office of Regulatory Compliance, Privacy and University Counsel before conducting research in the EEA. If you have any questions about GDPR and your research project, please contact COMIRB, Privacy or Legal Affairs.

What is GDPR?

GDPR is a European law that establishes data protections for privacy and security of personal data about individuals located in the European Economic Area (EEA).

How is GDPR different from other privacy laws like HIPAA?

GDPR is broader and more restrictive than HIPAA. For example, GDPR applies to all "personal data," whereas HIPAA applies only to Protected Health Information.

> "Personal data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural 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, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

GDPR involves severe fines for infractions. The most serious infractions are subject to administrative fines up to €20 million, or up to 4 percent of the total worldwide annual income of the responsible business party for the preceding financial year, whichever is higher.

GDPR requires notification to data protection authorities and affected individuals within 72 hours following the discovery of a personal data breach, which is a security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

GDPR establishes rights for an individual to have their personal data erased.

GDPR establishes additional restrictions related to "special categories" of personal data. "Special categories" of personal data include racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, or data concerning a person's sex life or sexual orientation.

Some specific ways GDPR impacts human subjects research

- GDPR requires investigators to obtain consent from subjects even if their research is exempted by the IRB, and in some situations, even if the research qualifies as not-human-subjects research.
- Data subject to GDPR may only be used for the purpose for which informed consent was provided.
- A data set that is "de-identified" under IRB and HIPAA standards may not be considered "anonymized" under GDPR. This means researchers may be required to submit an application to COMIRB for research which is not "human subjects research" under the Common Rule.
- Under GDPR, if a person who agreed to be in research asks that their data be erased, the researcher is obligated to do so. De-identifying the data would not be sufficient.
- Noncompliance with GDPR can result in severe fines for the researcher, the researcher's department and the University.
- GDPR requires researchers and the University to implement more stringent data security measures than those in place for HIPAA.

When does GDPR apply to research?

GDPR applies to activities within the borders of EEA countries, that are related to offering goods or services to subjects within the EEA, or that involve monitoring the behavior of subjects within the EEA. Conducting research on human subjects who reside in the EEA falls under GDPR. This would include receiving data or biological specimens from residents within the EEA.

What countries are in the EEA?

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

* Although the United Kingdom is no longer part of the EEA, their corresponding privacy law (UK-GDPR) has the same requirements, so these guidelines also apply to our research involving data from the UK.

Additional requirements for consent

GDPR requires a legal basis to collect and process (*i.e.*, analyze) personal data. The legal basis that generally will apply is consent from the subject.

Consent must be freely given, specific, informed and unambiguous as to the subject's wishes by a statement or by a clear affirmative action. In many ways this is consistent with Common Rule requirements for informed consent. However, there are some subtle and critical differences, such as the following:

- *Specific* under GDPR means that researchers must obtain consent for each use of the subject's data separately. If the research involves sub-studies, each sub-study requires separate documentation of consent. A single signature at the end of the consent form for a study with multiple purposes is not sufficient.
- *Unambiguous* under GDPR means that subjects must clearly choose to enroll in the research. "Silence, pre-ticked boxes or inactivity should not therefore constitute consent." In other words, opt-out or implied consent procedures would not satisfy GDPR.
- The consent must be written "in an intelligible and easily accessible form, using clear and plain language." The plain language requirement means the consent may not include technical jargon or legalese. The clear language requirement means that "language likely to confuse — for example, the use of double negatives or inconsistent language — will invalidate consent."
- Researchers must make it easy for subjects to withdraw consent.
- Researchers must be able to demonstrate that a particular subject consented to the research. Consent records, including time and date of consent, must be maintained for each data subject.
- There is no ability for the IRB to waive informed consent under GDPR. If the IRB determines that the research is exempt, informed consent will still be required under GDPR.

This is not an exhaustive list of consent requirements under GDPR.

Data Security

Data protection measures that are HIPAA compliant are not necessarily GDPR compliant. Additional review and technical solutions for any data collected under GDPR will be required.

Standards for Anonymization

GDPR has extremely high standards for anonymization: "Removing directly identifying elements in itself is not enough to ensure that identification of the data subject is no longer possible."

GDPR compliance is still required for research involving coded ("pseudonymized" under GDPR) data from residents in the EEA.

Contacts

This guidance provides a summary of many of the important issues imposed by GDPR, but it is not an exhaustive description of GDPR. If you are considering research involving the EEA, contact COMIRB, the Privacy Officer, or University Counsel.

Links to More Information

- University of Colorado OIS Guidance
- Complete guide to GDPR compliance