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 requires compliance with GDPR. This impacts researchers seeking to interview or survey subjects in the EEA, even if traditional identifiers are not collected. This also impacts researchers conducting secondary research on de-identified data or biospecimens from EEA residents.

Review Process for GDPR

- Research must be reviewed by COMIRB and a GDPR committee.
- Submit an application to COMIRB, even if you are not receiving traditional subject identifiers.
- Clearly identify any involved institutions from the EEA in the Application and protocol.
- COMIRB and/or the Privacy office will contact you to develop an SOP for managing and protecting your data.
- After confirming a need for GDPR compliance, the PI, and any research personnel with access to the GDPR data must complete the first module ("GDPR Overview") of the CITI "GDPR for Research and Higher Ed" course.
- The GDPR Committee will review the project and data security plans. If approved, the PI will be asked to sign the SOP, COMIRB will complete our review, and any contractual agreements will be finalized.
- For questions, contact COMIRB or the Privacy Office.

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).

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). If your research can be conducted without involving the EEA, we encourage you to adopt that strategy.

GDPR Committee

For research with data or contracts that require GDPR compliance, an additional GDPR committee must review the study and data security plans to ensure the University is in compliance with GDPR. The GDPR committee includes representatives from COMIRB, Privacy, Office of Regulatory Compliance, University Counsel, and OIT.

Researchers typically do not have to submit any materials directly to the GDPR committee, nor will they receive approval letters from the GDPR committee. Rather, communication is managed by members of the GDPR committee back to the researcher, COMIRB, Privacy, and/or University contracting officials.

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 infractions involve severe fines. 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 that 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?

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

*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.
- The IRB cannot grant a waiver of informed consent under GDPR. Even if the IRB determines that the research is exempt, informed consent will still be required under GDPR.

COMIRB can provide GDPR compliant template language to add to the consent form.

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.

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. COMIRB and/or the Privacy office will contact you to develop an SOP for managing and protecting your GDPR data. To ensure GDPR is followed, the SOP will specify how data will be transferred, stored, and used, who will have access, which software services you will use, etc.

Education

For research that requires adherence to GDPR, the PI, and any research personnel with access to the GDPR data must complete the first module ("GDPR Overview") of the CITI "GDPR for Research and Higher Ed" course and send an email to privacy@cuanschutz.edu when completed.

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 Office, or University Counsel.

Links to More Information

- CU Denver | Anschutz Medical Campus Privacy Office
- University of Colorado OIS Guidance
- Complete guide to GDPR compliance