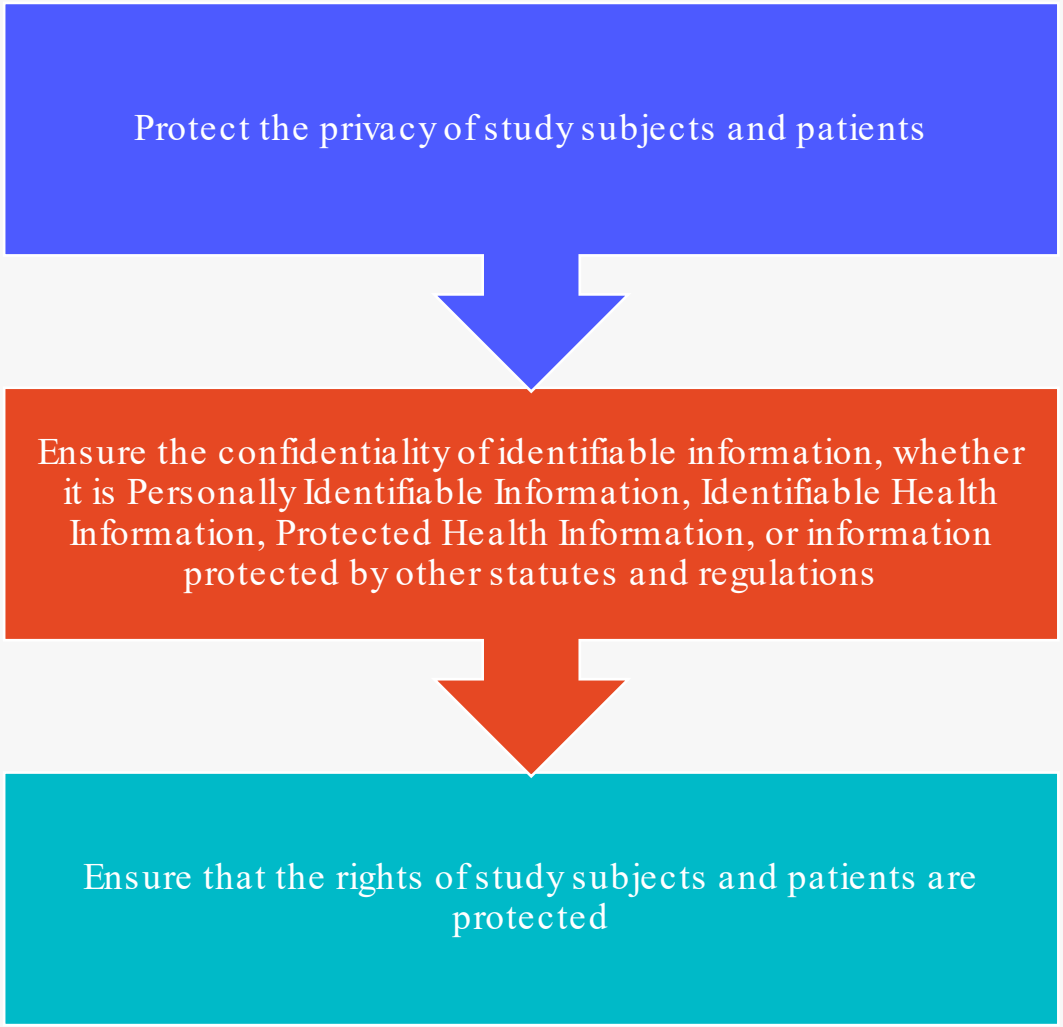
Research Privacy Information and International Data Protection Law Updates

Tracy Dawson, JD, RN

Director of Privacy Initiatives and Privacy Officer

Office of Ethics and Compliance

The Role of Privacy and Data Protection in Research



The Privacy Officer

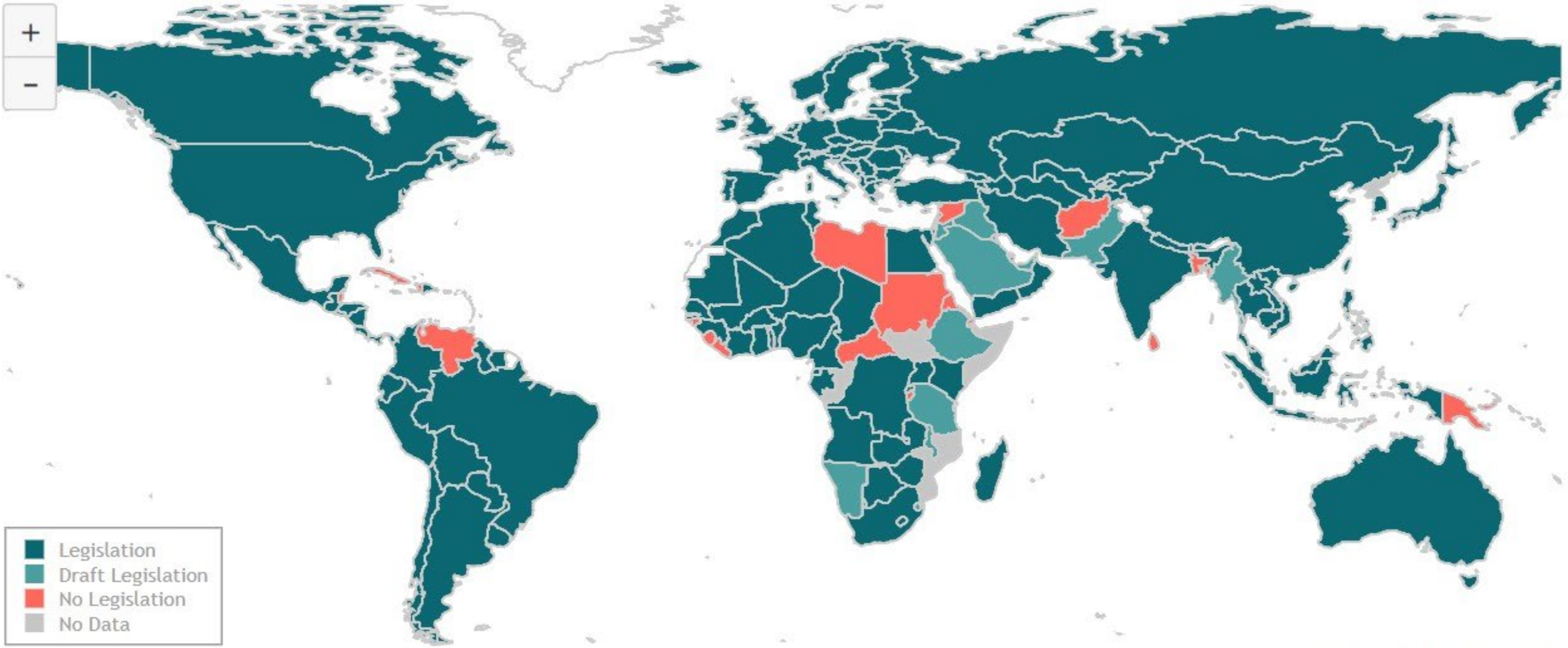
In general, the role of the Privacy Officer is to ensure compliance with state, federal and international privacy and data protection laws throughout the University. This requires collaboration with other offices that have similar or related responsibilities.

Collaboration with ORA, the IRB, PIs, study teams and other stakeholders

- Provide guidance on issues as they arise in connection with HIPAA, FERPA (rare in research), GINA (anti-discrimination), Georgia state laws on HIV and mental health information, international privacy and data protection laws, and the new state privacy laws
- Provide guidance to the IRB on issues that have a privacy component, especially where privacy and research regs are both involved
- Review agreements such as Data Use Agreements, Data Protection Agreements, Joint Controller Agreements, European Union Standard Contractual Clauses, Business Associate Agreements
- Conduct investigations into “privacy incidents”, which may or may not be actual breaches
- Work with the Emory Healthcare Office of Compliance Programs on finding solutions to the many issues involved in providing University researchers access to EHC PHI.

Global Privacy Laws

Data Protection and Privacy Legislation Worldwide



Source: UNCTAD, 14/12/2021

Most Applicable International Privacy and Data Protection Laws and Regulations

EU GDPR (the European Union General Data Protection Regulation)

UK GDPR (the United Kingdom General Data Protection Regulation)

PIPL (the Chinese Personal Information Protection Law)

PoPIA (South Africa's Protection of Personal Information Act)

EU GDPR and UK GDPR

The EU GDPR is the data privacy and security regulation that went into effect in May of 2018. Its purpose is to impose strict data protection requirements on the use of the personal data of individuals LOCATED IN the European Union. Residency or citizenship is not a requirement.

The EU GDPR applies to individuals located in the 27 countries of the European Union and Norway, Iceland, and Lichtenstein – together, the European Economic Area (EEA). Please note, Switzerland is not part of the EEA.

After exiting from the European Union, the United Kingdom made the decision to adopt its own General Data Protection Regulation, which is essentially the same law as the EU GDPR, but with changes to accommodate domestic areas of law. It went into effect on January 1, 2021.

The GDPR will usually apply to a research study or project when…

- Research is being conducted in the EU/UK or study subjects are recruited in the EU/UK.
- A component of a research project, especially a clinical trial, is conducted in the EU/UK and data is transferred to the United States.
- Research is sponsored by a company that is located in or has establishments located in the EU/UK. These companies may even require Emory to comply with the EU/UK GDPR even if the study subject information is from American subjects and being transferred to the EU, where the GDPR does not apply as a matter of law.

Key Point

The European Union and the United Kingdom DO NOT recognize the United States standard of de-identification. The only Personal Data that is not subject to the GDPRs is **anonymized** Personal Data, which is a much more difficult standard to meet than de-identified. It is defined as

…“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.”

The PIPL

The Personal Information Protection Law was implemented in China effective November 1, 2021. It is similar to the EU GDPR in many respects. It imposes a broad set of data privacy requirements on the processing of personal information about individuals LOCATED IN the People's Republic of China.

Applicability of the PIPL

The PIPL applies to all activities that involve the handling of the Personal Information of natural persons **located within borders** of the PRC.

In the following circumstances, the PIPL also applies entities outside of the PRC who are handling the of personal information of natural persons within the borders of the People's Republic of China:

- Where the purpose is to provide products or services to natural persons inside the borders
- Where analyzing or assessing activities of natural persons inside the borders
- Other circumstances provided in laws or administrative regulations

As a practical matter, the PIPL will apply to a research study or project for one or more of these reasons:

- Research is conducted in China or study subjects are recruited in China.
- A component of a research project is conducted in China and data is transferred to the United States.
- Research is sponsored by a company in China.

BUT, keep in mind that, unlike the European Union or any of its Member State governing bodies, the Chinese government can insert itself into anything and everything involving data regulation.

PoPIA

The Protection of Personal Information Act ("PoPIA") was implemented in South Africa on July 1, 2020. It is designed to protect the privacy of individuals by regulating the processing of their personal information.

Applicability of PoPIA

The PoPiA applies to the processing of personal information in various contexts, including research activities.

Key considerations for research:

- PoPIA applies when researchers collect, use, store, or otherwise process personal information. Personal information includes any information that can identify an individual.
- If the research involves the processing of personal information of individuals in South Africa, PoPIA is applicable.
- Researchers must obtain the consent of the individuals whose personal information is being processed, unless an exemption or condition for lawful processing applies.
- Processing of “Sensitive Personal Information,” such as health information or information about race or ethnic origin, are considered sensitive and is subject to stricter requirements.
- Personal information collected for research purposes should only be used for the specific research objectives and not for other unrelated purposes.

Privacy Updates

- On August 9, 2023, India passed the Digital Personal Data Protection Act ("DPDP"), which applies to the processing of digital personal data within the territory of India collected online or collected offline and later digitized.
- On September 1, 2023, the Revised Federal Act on Data Protection (FADP) Act in Switzerland went into effect and essentially implements stricter rules on the processing of personal data.
- AI Regulations
  - On 15 August 2023, China implemented new AI regulations designed to regulate generative AI, address risks related to AI and introduce compliance obligations on entities engaged in AI-related business.
  - On October 30, 2023, the White House issued an Executive Order on AI that establishes "new standards for AI safety and security, protects Americans' privacy, advances equity and civil rights, stands up for consumers and workers, promotes innovation and competition."
  - Earlier this month, the US Senate held the Sixth Bipartisan Senate Forum On Artificial Intelligence which focused on the issues of privacy and liability in AI.
  - The EU's AI Act, currently in negotiations, is expected to pass and could apply to businesses as soon as 2025.
  - Existing regulations, such as the GDPR and the EU's Digital Services Act, could also be adapted to incorporate provisions around AI.

Contact Information

Tracy Dawson, JD, RN

Director, Privacy Initiatives and University Privacy Officer

Tracy.s.Dawson @emory.edu

Phone: 404.727.4904

Office of Ethics and Compliance

Compliance@emory.edu

404.727.2398