Evaluating Health Data Regulations in the Era of Advanced Technologies: A Focus on Mental Health Data Ethics

Fedora Castelino; Michael Kiel; Laura Wang; Sandra E. Yankah, Ph.D.

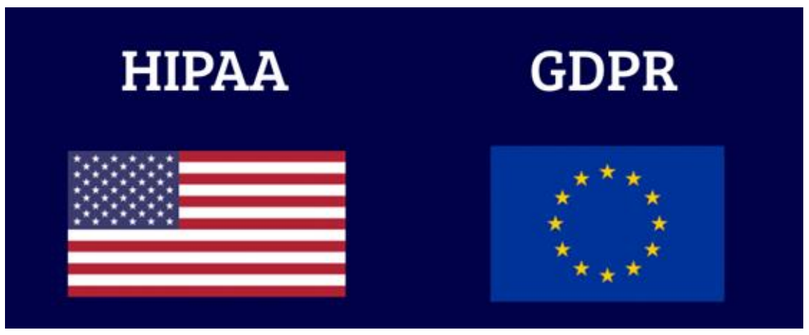
Duke | MARGOLIS CENTER for Health Policy

Introduction/Background

ESTABLISHING THE FRAMEWORK: HEALTH DATA REGULATIONS AND MENTAL HEALTH ETHICS IN FOCUS

Health data regulations are foundational to ensuring the privacy and integrity of sensitive information, with particular significance in the domain of mental health data. As the custodians of patient well-being continue to navigate the evolving landscape of healthcare, two pivotal regulations, HIPAA and GDPR, stand as pillars in safeguarding health data. Recognizing the profound impact of technological advancements, this research delves into the critical intersection of health data regulations and mental health ethics.

The overarching objective of this project was to rigorously evaluate current health data regulations, focusing specifically on their adaptability to the rapid evolution of technological capabilities. By scrutinizing the effectiveness of existing frameworks, this study aimed to provide insights into the strengths and limitations of regulatory measures in safeguarding the ethical use of mental health data within an era dominated by advanced technologies.



Methods

Our methodology involved a targeted analysis of specific aspects of health data regulations, focusing on the contrasting features of HIPAA and GDPR. To achieve this, we systematically reviewed legal documents pertinent to HIPAA and GDPR, extracting key details related to 13 domains including:

- Scope
- Consent requirements
- Data subject rights
- International data transfer protocols
- Purpose limitation
- Governance
- Provisions for children's data privacy
- Definition of mental health data
- Data minimization practices
- Security mandates
- Penalties for non-compliance
- Accountability
- Data breach notifications

This comprehensive examination ensured a detailed understanding of how each regulation addresses these critical dimensions, forming the basis for our subsequent comparative analysis.

Results

Our comparative analysis of HIPAA and GDPR provisions on mental health data reveals distinct regulatory approaches with profound implications for the safeguarding of sensitive information. HIPAA, focusing primarily on health information within the U.S., defines mental health data implicitly within the broader category of PHI. In contrast, GDPR, extending its global reach, classifies mental health data under "Special Categories of Personal Data," showcasing a comprehensive approach to the unique sensitivity of mental health information. GDPR grants individuals enhanced data subject rights: the right to be forgotten, data portability, and the right to object to processing, providing a more nuanced control over personal mental health data. On the other hand, HIPAA emphasizes the minimum necessary use and disclosure of PHI, showcasing a cautious yet domestically centered approach. The security requirements of GDPR, coupled with stringent breach notification mandates, underscore its commitment to safeguarding mental health data on an international scale.

Comparison Chart: HIPAA vs. GDPR - Key Provisions on Mental Health Data

Domain	HIPAA	GDPR
Scope	Covers health information in the U.S.	Applies to personal data in the European Union and beyond
Definition of Mental Health Data	Defines Protected Health Information (PHI) but doesn't explicitly specify mental health data	Defines "Special Categories of Personal Data," explicitly mentioning mental health data
Consent Requirements	Requires informed consent for the use and disclosure of health information	Emphasizes explicit consent and provides specific requirements for sensitive data, including mental health information
Data Minimization	Promotes the minimum necessary use and disclosure of PHI	Encourages data minimization, limiting the processing of personal data to what is necessary
Data Subject Rights	Grants individuals the right to access their health information and request corrections	Provides enhanced rights, including the right to be forgotten, the right to data portability, and the right to object to processing
Security Requirements	Requires covered entities to implement safeguards to protect health information	Mandates a higher level of security measures and breach notification requirements
International Transfer	Generally does not address international data transfers explicitly	Requires mechanisms such as Standard Contractual Clauses for transferring data outside the EU
Penalties for Non-compliance	Imposes civil and criminal penalties for violations	Imposes severe fines, up to 4% of annual global turnover or €20 million, whichever is greater
Purpose Limitation	Limits the use or disclosure of PHI to the minimum necessary for the intended purpose	Requires that personal data be collected for specified, explicit, and legitimate purposes, and not further processed in a manner incompatible with those purposes
Accountability and Governance	Emphasizes the need for covered entities to have policies and procedures in place to ensure compliance	Requires organizations to demonstrate compliance, implement data protection policies, and conduct impact assessments, promoting accountability
Data Breach Notification	Mandates covered entities to notify affected individuals, the Secretary of Health and Human Services, and, in some cases, the media in the event of a breach	Requires organizations to report data breaches to the supervisory authority within 72 hours, and in certain cases, notify affected individuals
Children's Data	Contains provisions for the protection of the privacy of minors' health information	Requires special protection for children's data and may necessitate parental consent for processing such data

Sources

Office for Civil Rights. “HIPAA for Professionals.” *HHS.Gov*, 16 Aug. 2021, www.hhs.gov/hipaa/for-professionals/index.html.

“What Is GDPR, the EU’s New Data Protection Law?” *GDPR.Eu*, 14 Sep. 2023, gdpr.eu/what-is-gdpr/.

Discussion

The findings underscore the need for a nuanced understanding of how regulations address mental health data in an increasingly globalized landscape. GDPR's expansive scope and robust data subject rights reflect a comprehensive approach to privacy, demanding a reevaluation of how U.S. regulations such as HIPAA adapt to international standards. The emphasis on explicit consent in GDPR contrasts with HIPAA's focus on informed consent, highlighting the evolving expectations for transparency in data processing. These differences necessitate ongoing discussions regarding harmonization of global privacy standards and the potential impact on healthcare practices.

Implications & Recommendations

IMPLICATIONS OF FINDINGS:

The implications of our research extend to policymakers, healthcare practitioners, and stakeholders navigating the intersection of mental health data, technology, and ethics. Policymakers must consider potential adjustments to domestic regulations to align with international standards. Healthcare practitioners need to be aware of the divergent requirements under HIPAA and GDPR, ensuring compliance and ethical practices in the increasingly interconnected healthcare landscape. Stakeholders should engage in ongoing dialogues to shape evolving regulations that balance patient privacy, technological innovation, and global data exchange.

POLICY RECOMMENDATIONS:

- There is a pressing need for a harmonized approach to mental health data regulations globally, considering the interconnected nature of healthcare and data exchange.
- Policymakers should explore mechanisms for aligning domestic with international standards, fostering a unified framework for mental health data protection.
- Continuous efforts should be made to enhance transparency and consent mechanisms, acknowledging growing expectations for control over personal data.
- Policymakers should consider ongoing education initiatives for healthcare practitioners to ensure a comprehensive understanding of the evolving regulatory landscape and its implications for the ethical use of mental health data.

ACKNOWLEDGMENTS: Special thanks to Dr. Yankah, Dr. Hendricks Stirrup, Dr. Sloan, Ms. Nafie, Ellen Zeng, Cassie Liang, Nate Einfeldt, Riya Mohan, and the Duke Margolis Center of Health Policy. Health Data Science at Duke is supported by the National Center For Advancing Translational Sciences of the National Institutes of Health under Award Number UL1TR002553. The Duke Protected Analytics Environment (PACE) program is supported by Duke’s Clinical and Translational Science Award (CTSA) grant (UL1TR001117), and by Duke University Health System. The CTSA initiative is led by the National Center for Advancing Translational Sciences (NCATS) at the National Institutes of Health.

DukeHealth

Health Data Science Poster Showcase

Duke University, December 8, 2023