The Case for Increased Health Privacy in Digital U.S. Markets

Abstract

The rapid advancement of digital health technologies, including wearable devices, mobile health applications, and telemedicine platforms, has revolutionized healthcare by enabling personalized care, remote monitoring, and real-time health tracking. While these innovations enhance patient outcomes and engagement, they also present significant privacy challenges. Unlike traditional healthcare entities regulated under the Health Insurance Portability and Accountability Act (HIPAA), technology companies operating in the digital health space often fall outside this regulatory framework. As a result, vast amounts of sensitive health data collected by these entities remain inadequately protected, exposing consumers to potential misuse and security risks.

This paper critically examines the limitations of existing U.S. privacy frameworks, particularly HIPAA and the Federal Trade Commission (FTC) Act, in addressing the unique privacy vulnerabilities of digital health data. It explores the regulatory gaps that allow non-HIPAA-covered entities to collect, store, and share personal health information without uniform oversight or accountability. Furthermore, it evaluates industry practices that contribute to these privacy concerns, such as inconsistent consent mechanisms, varied data security requirements, and the absence of comprehensive consumer rights regarding data access and portability. Through this analysis, the study highlights the pressing need for a more robust and cohesive federal policy framework.

To address these deficiencies, this paper proposes a comprehensive legislative approach that ensures enhanced consumer protection while fostering continued innovation in digital health technologies. Drawing on international regulatory models such as the European Union's General Data Protection Regulation (GDPR), the study identifies best practices that could inform U.S. policy reforms. By integrating evidence-based recommendations, including standardized data governance mechanisms, strengthened consent protocols, and enforceable consumer rights, this paper advocates for a modernized legal framework capable of safeguarding digital health data in an increasingly interconnected and technology-driven healthcare landscape.

KEYWORDS: Mobile Health, Data Privacy, Consumer Protection, Policy Gaps, Wearables, Federal Legislation, Data Security, Federal Trade Commission (FTC) Act, Health Insurance Portability and Accountability Act (HIPAA), General Data Protection Regulation (GDPR)