CASE STUDY: WEARING DOWN HIPAA: HOW WEARABLE TECHNOLOGIES ERODE PRIVACY PROTECTIONS

Steve Desilets

MSDS 485: Data Governance, Ethics, and Law

November 19, 2023

1. Introduction

While the US federal government has taken strong steps to protect Americans' personal health information (PHI) via the Health Insurance Portability and Accountability Act of 1996 (HIPAA), producers of wearable health technology often are not subject to this law's rules. As John T. Katuska points out in "Wearing Down HIPAA: How Wearable Technologies Erode Privacy Protections," this gap in legal protections raises risks for both consumers and technology companies (Katuska 2018). Specifically, consumers are at risk of wearable health tech companies selling their PHI to third parties, including third parties that might use the information in ways that detrimentally impact the consumers. Meanwhile, producers of wearable health technology currently exist in a state of legal limbo causing them to not know whether they truly need to undertake costly projects to comply with HIPAA or whether they'd even be liable for HIPAA's severe financial and criminal penalties for violations. In this paper, we discuss the data, data governance, relevant legislation, and data governance solutions presented in this case study that advocates for legislation that would provide protections for consumers of wearable health technology and unambiguous regulatory guidance to producers of these devices.

2. The Data

The data upon which this article focuses is health data collected by companies that create wearable technology. Common examples of such data include information about consumers' heart rates, steps, and sleeping patterns. The author specifies that the data of particular interest is data collected while doing business primarily with a consumer – not data collected while primarily doing business with a HIPAA-designated covered entity, such as a healthcare provider. As the author explains, most of the data collected by these companies falls into the former category and consequently is not subject to HIPAA. While the data and analyses collected by these technologies are likely sufficient for the purposes of creating pleasant visualizations that help consumers better understand basic health information, the author raises important questions about the privacy and security of this data.

3. Relevance To Data Governance

Within the context of the data governance framework defined by Eryurek et al. in *Data Governance: The Definitive Guide*, the focus of this case study most closely aligns to the "Policies" data governance framework component (Eryurek et al. 2021). Similarly, of the four Pillars of Data Governance (data stewardship, data quality, master data management, and data governance use cases), this article primarily relates to the Data Stewardship Pillar, which implements policies related to data management, legal compliance, and ethics (Eye on Tech 2020). The reason that this case study so closely relates to data governance policies and data stewardship is that the author's

primary call-to-action is for the US government to expand HIPAA to apply to producers of technology for which the primary purpose is to collect consumers' health data, so that such companies will be forced to abide by data governance policies that better protect consumers' PHI.

4. Relevant Legislation

In Katuska's piece, HIPAA's Privacy Rule and Security Rule take center stage as the author outlines the protections these rules provide to the public, the types of organizations subject to these rules, and the types of data to which these rules apply. As the author explains, HIPAA's Security Rule mandates that certain organizations must establish robust technical, administrative, and physical safeguards to protect electronic PHI. Furthermore, HIPAA's Privacy Rule states that certain organizations must defend patient PHI via specific measures, such as securing patient records, designating a Privacy Officer, and never improperly disclosing patient PHI to third parties. However, Katuska continues the piece by explaining that the reason that wearable healthcare technology companies do not need to abide by the HIPAA Privacy and Security Rules is these companies usually would not meet the definition of a "covered entity" or "business associate" – the two types of organizations to which these HIPAA rules apply. This legal loophole means that consumers' deeply personal PHI collected by wearable devices may not protected with the same level of privacy and security that most Americans would expect – leaving consumers increasingly vulnerable to negative impacts of the sale or breaches of this data.

5. Data Governance Solution

As John T. Katuska points out, the current legislative landscape surrounding wearable healthcare technology creates ethical, privacy, security, and financial risks for consumers and businesses. Furthermore, the author astutely portends that these risks will only increase over time as new wearable consumer technologies to measure more health metrics (such as blood sugar, blood alcohol content, and muscle activity) emerge. Consequently, Katuska proposes that the US federal government expand the scope of HIPAA to apply to producers of wearable technology for which the primary purpose is collecting consumers' health data. The passage of such legislation would effectively mitigate security and privacy risks for both consumers and producers of wearable healthcare devices.

References

Eryurek, Evren, Uri Gilad, Valliappa Lakshmanan, Anita Kibunguchy-Grant, and Jessi Ashdown. 2021. *Data Governance: The Definitive Guide*. Sebastopol, CA: O'Reilly Media.

Eye on Tech. 2020. "What is Data Governance? How Does it Impact Businesses?" YouTube, 2:16. February 14, 2020. https://www.youtube.com/watch?v=BqdPuwvwPk4

Katuska, John T. 2018. "Wearing Down HIPAA: How Wearable Technologies Erode Privacy Protections." *The Journal of Corporation Law* 44 (2): 385 – 401.