

Spring 2021

The Impacts of Health Information Being Shared on Social Media Platforms by Healthcare Providers

Vivine Ishimwe

United States Coast Guard Academy, Cyber Systems Major

Vivine Ishimwe@uscga.edu

Abstract

The rapid development of the use of communication technologies and social media among healthcare providers raises potential privacy issues for patients. Health Information can be easily transmitted using platforms like Facebook, Instagram, Twitter, Snapchat, and TikTok that allow users to communicate electronically with friends and family all over the world. Thus, offering means of spreading sensitive healthcare information—as well as an easy way to compromise patient privacy. the purpose of this research is to shed light on how medical information shared on social media by healthcare providers poses risks to patient's privacy in the United States. To better explain and understand the research problem, both qualitative and quantitative methods were used. These include scientific facts, statistics, surveys, interviews, social media posts, and studies conducted from 2000 to 2021. Also, all quantitative data used were taken from the existing literature done by other researchers. Before conducting the research, the expectations were to use primary data to better show the existing gap and explain the research problem. However, due to some limitations, many assumptions and analyses were made based on secondary data. This research paper will help healthcare professionals to improve in ways that are "privacy-respecting and privacy reinforcing.

Keywords- Patients , Healthcare, Privacy, Social Medias

# I. INTRODUCTION

According to Statista reports, one of the most common online practices is social media, and in 2021, 82 % of the American population have a social networking profile. This adds up to nearly 223 million social media users in the United States. Among the users, there are healthcare providers who use social media daily, and there is no indication that this will change. Although it is pleasant and relaxing it raises the possibility of privacy issues. For example, more than 56 percent of the 4.5 billion leaked data in the first half of 2018 came from employees who posted patient's confidential health information (PHI) on social media, resulting in HIPAA violations. Some of the incidents were unintentional while others were for education, views, and money. Perhaps PHI was hiding in the background. But regardless of the situation, PHI should neither be discussed nor posted because it negatively affects the patient. This research paper aims to show the impacts of health information being exposed on social media platforms by healthcare providers and provides policies that should be put in place to preserve patient’s privacy. Furthermore, this research will improve the doctor-patient relationship and will help to protect patient’s rights and interests.

# II. METHODOLOGY (EASE OF USE)

The methodology used in this research is mixed. The data collected are from the existing literature and are both quantitative and qualitative. During the development of the research problem case studies, surveys, statistics, articles, academic journals, and social media posts in the health care and information communication technology field were examined to select appropriate sources.

Quantitative Method

The quantitative method is the process of gathering and examining numerical data. This method was used to find and analyze patterns between statistics provided by different researchers on the related topics.

Qualitative Method

The quantitative method is the opposite of the qualitative method, which involves gathering and examining non-numerical data. This method was used to gather information from texts and video logs posted on social media.

In conducting this research, neither interviews nor surveys were conducted by the author. All data used were based on the existing literature and observation from social media posts. Furthermore, limitations such as time, method, access to literature cases, age of data provided, and timing of the studies affected the data collection process.

Time: There was a deadline to turn in each section of this research paper. This limited the data collection process and some of the information was left behind to meet the due dates.

Access to literature cases: United States Coast Guard Academy library does not provide access to all literature cases and this affected my research because I needed access to the existing cases to identify the gap, understand, and explain the research problem I was trying to address.

Age of data provided: Some of the assumptions made are based on the secondary data.

Timing of the studies: Some case studies are a decade old, and some assumptions did not consider the advancement made after those studies were published.

By using both methods, the limitations of one method balance the other one. For example, qualitative data like TikTok videos whose credibility might be questioned were balanced by the strength of quantitative data like statistics obtained and this helped to better improve the understanding of the research problem.

**Cases where patients were impacted by their healthcare provider’s social media posts**

Three male employees at Glencroft Senior Living facility in Glendale, Arizona were fired in November 2017 after they were accused of videotaping elderly patients and uploading their videos on Snapchat stories. Employees in the video are seen making fun of elderly residents in their care, and instead of helping one woman who has requested assistance, the employee laughed at her and proceeds to film the situation. Due to their actions, this patient with dementia was not able to get her medicine on time and the video shows that she was very distressed and nervous that someone was filming her medical condition to the public.

A similar incident happened in February 2021. In a video posted on TikTok, a woman suffering from a sexually transmitted disease shared her story explaining how she was exposed by her doctor. The patient claimed that the doctor used information from her medical records to make the video logs that he posted on Facebook and YouTube. She continued by saying that this doctor stalked her Facebook profile and was able to share the Vlog with the patient’s friends. Days after the incident, people started asking sensitive questions about the patient’s diseases which put her in a distressed situation. This woman said,” his posts completely affected my mental health, I wonder what my friends think of me now, I feel violated and helpless”.

# III. FINDINGS

The above incidents and many others that cannot be covered in this paper highlight the importance of having protocols and measures in place which ensure that the privacy of patients is preserved in the healthcare sector. Taken from the Institute of Electrical and Electronics Engineers publication, the study shows that 84 percent of patients have directly encountered negative effects as a result of personal data leakage by their healthcare providers. The exposure of this sensitive information has resulted in both social and psychological damage to the patients. These include bullying, suffering from mental health issues, patients losing their jobs, and patients stopping from seeking care.

**Bullying**

In the survey done by senior medical students from Arizona, a total of 100 of 169 patients (59.17%) responded. In 100 patients who responded, 17.2% reported that they have been bullied as a result of their medical conditions exposure. Also, in 2020, BBC covered a story about an HIV-infected patient who was constantly being harassed by his family members after finding out that he is infected. The family members found out from the Facebook group after the nurse allegedly showed the patient’s records in her vlogs. As a result of bullying, many patients suffer from mental health issues such as depression, sleep disorder, anxiety, and many others.

**Mental health issues**

Patients suffer from mental health issues as a result of their PHI being exposed to social media. According to the Centers for Disease Control and Prevention (CDC), “Mental illnesses are conditions that affect a person’s thinking, feeling, mood or behavior, such as depression, anxiety, bipolar disorder, or schizophrenia”. Most of the time, healthcare providers take patients' pictures/videos and write blogs that mention patient’s personal information that make it easier for other people to identify the patients. Many justify their actions by saying it is for educational purposes. However, these particular situations result in mental health issues upon the patient whose information was exposed. For example, in 2019, a surgeon named Dr. Mayer shared a video log on his Instagram about a patient who was doing breast enlargement. The video includes the patient’s body parts and also her face. Before the operation, the patient signed the consent that allowed the doctor to post the video for educational purposes. However, the patient did not know the specifics of the video. After the operation, the patient requested the doctor to not share the video, but the doctor shared it anyway. After three months, the girl was found dead due to suicide. The police report shows that after her surgery was shared on Instagram, her friends started bullying her for getting body surgery which caused her depression and made her took her own life.

There are so many cases like these that occur due to a single post shared by healthcare providers.

**Patients lose their jobs**

As a healthcare provider, posting patient’s information costs them their jobs. Some patients have diseases that prevent them from doing some particular jobs. But, due to financial problems, some chose to do them anyway. When their conditions are exposed, it forces them to resign from their jobs and in some cases get fired. Not only does this affect their financial status but also their social status.

**Patients stop seeking medical help**

Patients stop seeking medical help due to privacy concerns. The aftermath of privacy incidents is that patients lose trust in their healthcare providers and stop getting the help their need. Not only does this cause additional health problems, but it also results in death in some cases.

## Abbreviations and Acronyms

ICT: Information Communications Technology

IEEE: Institute of Electrical and Electronics Engineers

PHI: Patients Health Information

HIPPA: Health Insurance Portability and Accountability Act of 1996

VLOGS: Video Logs

EMT: Emergency Room Technician.

CDC: Center of Diseases

# IV. DISCUSSION

As of today, there are no concrete HIPAA social media rules since HIPAA was enacted many years before social media networks like Facebook, Instagram, Snapchat, and TikTok were launched; however, there are HIPAA rules and guidelines that relate to social media use by healthcare employees. Thus, everyone in the field must be aware of the rules and regulations of posting. i.e., what you can post and what you cannot. When using social media platforms healthcare professionals must respect patients' privacy rights by posting pictures, videos, and video logs that follow the Health Insurance Portability and Accountability Act of 1996 (HIPAA). They should do so by:

**Getting fully briefed consent from the patient**

In many cases, healthcare providers give less information to the patients regarding the consent form. This forces patients to sign things that they do not understand which later causes problems. To mitigate such issues, healthcare provides have to make sure that the patient fully understands what is going to be shared and the consequences it might cause. Moreover, healthcare workers must make sure that patients can neither be identified nor traced back that from their posts. This also includes avoiding post unprofessional images during the surgical process.

**Education regarding privacy**

Healthcare professionals should get lessons regarding patients’ privacy. They should be given training on how to use social media without exposing their patient's information. For instance, advising them to keep their professional and personal e-mail accounts apart wherever possible, and also improving their professionalism.

By using the above strategies, the negative impacts to patients caused by social media exposure can be mitigated.

REFERENCES

1. A. Algarni, A. “ A Survey and Classification of Security and Privacy Research in Smart Healthcare Systems,” IEEE Access, vol. 7, pp. 101879–101894.
2. A. Kaplan, “Electronic health records and patient privacy--an oxymoron?,” Psychiatric Times, vol. 29, no. 8, pp. 6.
3. A. O'Dowd, “MEDICAL DATA: Does patient privacy trump access for research,” BMJ: British Medical Journal, vol. 347, no. 7924, pp. 20-21.
4. B. Matthew, “Privacy risks when using mobile devices in health care,” PubMed Central (PMC).
5. C. -L. Feng, Z.-C. Cheng, and L.-J. Huang, “An Investigation into Patient Privacy Disclosure in Online Medical Platforms,” IEEE Access, vol. 7, pp. 29085–29095.
6. F. F. Ozair, N. Jamshed, A. Sharma, and P. Aggarwal, “Ethical issues in electronic health records: A general overview. Perspectives in clinical research,” vol. 6, no. 2, pp. 73–76.
7. G. Brisson, and P. Tyler, “Medical Student Use of Electronic Health Records to Track Former Patients,” JAMA Internal Medicine, no. 176, pp. 1395-1397.
8. I. Wielawski, “Are Patient Privacy and Health Data at Risk?,” AJN, American Journal of Nursing, no. 120, pp. 19-20.
9. M. A Azad, J. Arshad, S. Mahmoud, K. Salah, and M. Imran, “A privacy‐preserving framework for smart context‐aware healthcare applications,” Transactions on Emerging Telecommunications Technologies, no. e3634.
10. M. D. Seckeler, B. M. Gordon, D. A. Williams, and B. H. Goldstein, “Use of Smart Technology for Remote Consultation in the Pediatric Cardiac Catheterization Laboratory,” Congenital Heart Disease, vol. 10, no. 6, pp. E288–E294.
11. M. U. Jassan, M. H. Rehmani, and J. Chen, “Differential Privacy Techniques for Cyber-Physical Systems: A Survey,” IEEE Communications Surveys & Tutorials, pp. 1–1.
12. S. Hosek, and S. Straus, “Privacy of Individual Health Information. In-Patient Privacy, Consent, and Identity Management in Health Information Exchange: Issues for the Military Health System,” pp. 19-30.
13. S. Wilson, “A bigger threat to patient privacy when doctors use Facebook,” Jme.bmj.com.
14. T. C. Rindfleisch, “Privacy, information technology, and health care,” Communications of the ACM, vol. 40, no. 8, pp. 92–100.
15. T. Livsey, “Post-it pitfalls: new technology makes it easy to breach patient privacy unwittingly,” Nursing Standard, vol. 23, no. 14, pp. 26.
16. T. M. Hale, “Privacy and Security Concerns in Telehealth,” Journal of Ethics | American Medical Association, Dec. 2014.
17. X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, “Healthcare data gateways: Found healthcare intelligence on the blockchain with novel privacy risk control,” Journal of Medical Systems, vol. 40, no. 10, pp. 1-8.
18. A. Kaplan, “Electronic health records and patient privacy--an oxymoron?,” Psychiatric Times, vol. 29, no. 8, pp. 6.

|  |
| --- |
| Photo |

**I**shimwe Vivine was born in Rwanda on 16th July 1999. Ishimwe is a second-class cadet currently majoring in Cyber Systems at the United States Coast Guard Academy.

3