


**Validating or Violating:
An Introspective Look on
How Health Information
is Shared Online**

By: Elsie Sheppard


**"Arguing that you don't
care about the right to
privacy because you have
nothing to hide is no
different than saying you
don't care about free
speech because you have
nothing to say."**

Edward Snowden




Health information is highly confidential and easily exploited. Doctors have patient confidentiality for a reason. Everyone has the right to keep their personal health information personal. However, in the internet era, health information has become easily accessible by third parties; people other than you and your healthcare provider can access your personal data. Health information is protected not only because it can be potentially embarrassing for some patients but also because it can be used against those patients and to the benefit of others.

This zine will examine how different technological advancements make personal health information less secure. The first section will discuss issues surrounding telehealth systems popularized during the COVID-19 pandemic. The second section will overview how people willingly give away their health information on social media platforms like Instagram and Reddit. And, the third section will look at how wearable technologies such as Apple watches and Fitbits collect vast amounts of personal health data. While some of these data-collecting technologies may seem inconsequential, much more can be done with your health data than you would think.



Security Issues With



The COVID-19 pandemic popularized online video platforms like Zoom and Telehealth systems with hopes of lessening the spread of the virus. People could attend work meetings and doctor's appointments online, allowing them to complete daily tasks from the safety of their homes. Telehealth systems are digital platforms that enable people to access and manage their health care online. Many telehealth systems include the option for video conferencing, the ability to look at test results, the opportunity to request prescription refills, and the choice to message with nurses. With moving doctors' visits and other health care needs online, privacy concerns regarding the security of personal health information have come to the forefront.

Security Breaches



Many telehealth systems are susceptible to hacking. When things happen over the internet, hacking is always possible. With more people using the internet and telehealth systems for their healthcare needs, telehealth systems generate a lot of health information, making them prime targets for cyber-attacks. Hackers can hack into the actual video stream of a patient's visit, listening in on private and confidential conversations between patients and health care providers [1]. Telehealth systems also use the cloud to store information, which can be susceptible to hacking and harvesting confidential data [2]. The information hackers can collect from telehealth systems includes names, emails, and medical records, including biometric data ranging from blood pressure and blood test results to prescription information to family medical history.

The data that hackers collect from telehealth systems is valuable on the black market [3]. Telehealth systems hold a lot of personal information, both health-related and non-health-related, in one place, making them more desirable than other information, such as credit card numbers [4]. This stolen information can be used for many different purposes, including blackmailing patients and identity theft [5].



Telehealth Systems

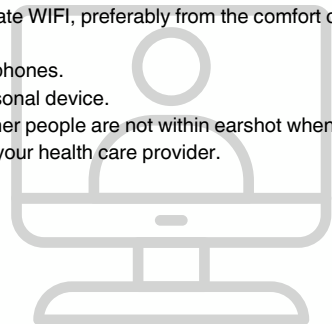
Cybersecurity firms and strategic design features can help to mitigate hacking and unauthorized data collection. Some design features that keep data more secure include two-factor or multi-factor authentication and regular system assessments to check for vulnerabilities [6].

Environmental Factors

Other security issues involve environmental factors or the location where an individual engages with telehealth systems. If an individual joins a telehealth video conference on a public WIFI, it makes them more susceptible to hacking. Private WIFI, like the ones in most homes, is more secure and ideal for telehealth conferencing. It is also essential to keep in mind who is around when using telehealth systems. People could be listening in on others' telehealth calls, whether that be other family members living in the same home or strangers if the call is taken in public.

Other environmental factors include giving your healthcare provider access to information they would not get with in-person visits, such as seeing your home through the background of your video. While this may not be harmful, some may consider blurring their background if they wish for extra privacy. Other ways to mitigate these environmental factors include:

- Using a private WIFI, preferably from the comfort of your home.
- Using headphones.
- Using a personal device.
- Ensuring other people are not within earshot when talking with your health care provider.



HIPAA Concerns

The Health Insurance Portability and Accountability Act (HIPAA) ensures that American citizens' health information stays confidential and is not used for unethical reasons. All telehealth systems must be HIPAA compliant to keep the information as safe as possible and lessen the possibility of cyberattacks. To be HIPAA compliant, telehealth providers must include a description of permitted and required uses of the data by the vendor (the ones providing the system), provisions that the vendor will not disclose health data other than what is stated in the contract, and the vendor must have some cybersecurity system to prevent the disclosure of health information [7]. HIPAA compliant systems include Skype for Business and Zoom for Healthcare.

HIPAA also provides privacy tips for healthcare providers. HIPAA suggests that providers should discuss privacy risks and precautions with patients who choose to use telehealth systems. Other tips for providers include reviewing privacy and security policies, scheduling the deletion of files on mobile devices, and utilizing data backup in case of a security breach [8].

While HIPAA has created guidelines about telehealth systems with the intention of protecting patient information, even with these safeguards in place, patient information is still susceptible to unauthorized collection by third parties.



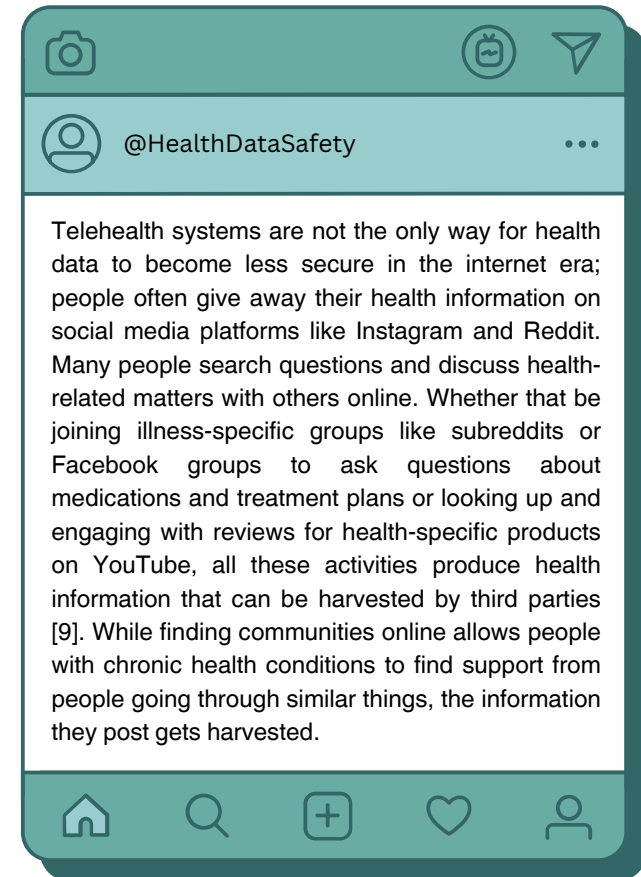
Benefits of Telehealth Systems

You may wonder, if telehealth systems cause so many problems, why do we continue using them? While telehealth systems do have drawbacks, these systems also have many benefits, including:

- Comfort. You can sit in the comfort of your home to attend appointments rather than physically going into an office. This is optimal for older patients and patients with a limited range of motion.
- Convenience and improved access. Finding a family doctor close to you is sometimes difficult, so telehealth visits help people save time from travelling to and from the doctor's office. Telehealth systems are particularly helpful for those living in rural areas.
- Control of spreading disease. As seen in the case of COVID-19, telehealth systems can lessen the spread of infectious diseases. People can access healthcare without putting themselves or others at risk of infection, which is particularly helpful for immunocompromised people.
- Reduced wait times. Doctors' offices usually have long wait times for getting an appointment and sitting in the waiting room. Telehealth allows doctors to fit more patients in during the day, and you won't have to wait in the sitting area with other sick people.

Telehealth systems have both benefits and drawbacks. However, it is hard to tell which one outweighs the other. Since telehealth systems are still in their infancy, it will take more time before we can truly decide if these systems are more beneficial or detrimental to society.

Security Issues With Social Media





Search Reddit

r/Rosacea · 3hr ago

Rosacea flare-up. HELPII

I have been experiencing a Rosacea flare-up recently. My dermatologist diagnosed me with type 2 Rosacea in 2017. I've tried so many treatments since then, including laser, ivermectin cream, azelaic acid cream, and Doxy/Cycline, but nothing seems to help. I would love to hear any success stories and learn what products you use to handle a flare-up.

2 0 Share

Add a comment

RainbowJusSubst1ner1302 · 13h ago

I find that creams with a gel-like consistency really help. I use Neutrogena Hydroboost, which is fragrance-free. Creams like this are really great for Rosacea and have worked well for me.

7 0 Reply Share ...

Skincarefan98 · 10h ago

I'm also experiencing a flare-up right now. I was diagnosed with type 1 and 2 three years ago. I've also tried all those treatments, but the one treatment that really helped was a small dose of propranolol. It's a blood pressure medication but can be prescribed off-label for facial flushing.

I got my dermatologist to prescribe it. I know not all doctors will, but mine has been great. If you live in the Greater Toronto Area, you should see Dr. Smith in Mississauga to see if he can prescribe it for you.

2 0 Reply Share ...

Skincarefan98 · 13h ago

Try buying a small hand-held fan to help with the heat from the facial flushing. This has really helped!

r/Rosacea

Rosacea

This is a mock Reddit forum to show you how much personal health information people post on social media.

Show more

67K Members 38 Online Top 2% Rank by size

COMMUNITY BOOKMARKS

Wiki

What information did they give away?

- 1 Medical Daignosis >
- 2 Perscription Information >
- 3 Personal Preferences >
- 4 Location Information >
- 5 Product Suggestions >

HIPAA Protections

The data one shares online falls outside of HIPAA protections. Whatever information you choose to share on your social media account is up to you. An individual can share all the information in their medical record online, with the hopes of getting help or relief from others, however, this information would not be under HIPAA protections. This means that the data can be collected and used without regulations put forth by the government; the interest of the patient is no longer at heart. The amount of personal health information shared online leads to “encroaching on the traditional doctor patient relationship and eroding medical privacy” [10]. By sharing medical information online, that information becomes insecure and available for anyone to see.

Data Brokers

Data brokers, companies that compile large quantities of data to sell to other parties, collect health information that people post online. Data brokers collect different kinds of information from all aspects of individuals’ internet use, including internet transactions and tracking data from smartphones [11]. The lists of individuals that data brokers compile can then be sold to other companies and are “available by diagnosis,” meaning that third parties can select personal health data sets based on specific health issues such as depression or anxiety [12]. This data can be used by companies for targeted advertisements for health products like experimental treatments and supplements.

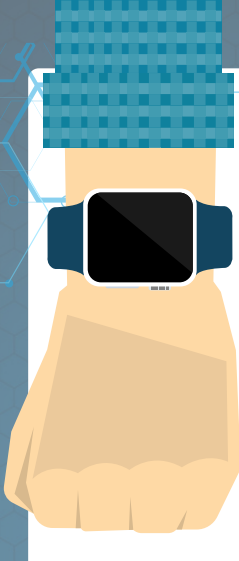
Targeted Advertisements

Social media platforms, such as Instagram, can also use the health information people post online for targeted advertisements, specifically health-related products. If people complain about or engage with content about a certain health issue they are experiencing, for example back pain, Instagram can target ads for products like heating pads, back rollers, and cooling gels.



Security Issues With Wearable Technology

Another way that third parties collect health data in the internet era is through wearable technology (WT) that tracks biometric data. WT refers to technology meant to be worn by a person, typically in the form of accessories such as watches, glasses, and other jewellery. Examples of WT include fitness trackers, smartwatches, and smart glasses. The most popular brands for WT are Apple, with the Apple Watch, and Google's Fitbit, with its various smartwatches. Fitbit's newest version, the Fitbit Sense 2, claims to help with stress management and sleep. Fitbit monitors the body whenever an individual wears the watch to improve these two health factors. By monitoring the body, the watch claims to identify when an individual feels stressed by providing stress notifications, offering stress management options, tracking sleep, and providing sleep and stress scores. The device also collects biometrics such as blood oxygen levels, heart rhythm, heart rate, skin temperature, breathing rate, and blood glucose levels. The Apple Watch offers similar services in addition to ovulation and cycle tracking. These devices seem to produce more health data than going to the doctor's office.



Wearable Tech “WT”

WT operates through small sensors and processors within the technologies. These devices can often connect to the internet, sync with other devices, and store an individual's health data in the cloud. Many of these WTs are associated with apps on different devices. Apple, for example, has a health app on the iPhone that can sync with the Apple Watch. Users can then track their health information from multiple devices.

While technologies like the Apple Watch and Fitbit are available for anyone wanting to monitor and take better care of their health, WT also helps individuals with actual health issues. WT for diabetics is quite common, with many people with diabetes wearing insulin pumps at all times. Insulin pumps are small devices that hold and distribute the correct amount of insulin to the body through a needle usually inserted into the stomach. The insulin pump is a lifesaving wearable device. The Continuous Glucose Monitor (CGM) is another wearable device for people with diabetes that accurately tracks blood glucose levels. The CGM is a small pod with a microneedle inserted into the skin, allowing the device to check blood sugar levels. This wearable device is more accurate at tracking blood glucose than the Fitbit. Wearable devices can not only motivate people to be more health conscious, in the case of people buying the Apple Watch or Fitbit, but also provide lifesaving technology, such as the insulin pump and CGM.

However, the amount of data these wearable devices collect threatens the security and confidentiality of personal health information. Fitbit claims not to share any personal information except for limited circumstances, which include when one gives consent by having certain privacy settings, for external processing (the information is sent to corporate affiliates for things like research and analysis), and for legal reasons [13]. The point of concern here comes at the external processing step, where Fitbit sends health information collected through its devices to third parties that can see and use the data. People who wear a Fitbit often have no idea who these third parties are or what actually constitutes 'research' and 'analysis,' as per Fitbit's privacy policy.

Fitbit Sense 2



Image taken from Fitbit's website: <https://www.fitbit.com/global/en-ca/products/smartwatches/sense2>

The Apple Watch



They know the health of your heart

They know exactly how you exercise

They know your sleep schedule

Since WT can connect to other devices through the internet or Bluetooth, these insecure wireless connections also make health information gathered on these devices susceptible to hacking and cyberattacks. Other privacy concerns about WT include GPS tracking by large companies like Google and Apple. Since Apple Watches and Fitbits track steps and routes, these conglomerates have access to where people are on a daily basis [14]. While wearable technology can be beneficial for people wanting to take better care of their health or who have medical conditions, it can also collect and track health data, making personal health data insecure.

Images taken from Apple's website: <https://www.apple.com/ca/watch/why-apple-watch/>

Tips to keep health data more secure

Try some of these out if you're worried about your privacy...

Look at the privacy settings on your health apps and wearable technologies. Sometimes, they have options for increased security.

Password protection. Create strong passwords for your social media and telehealth accounts.

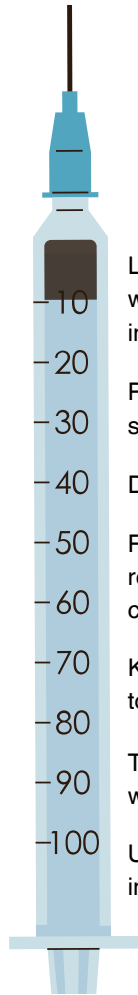
Do not use a public WIFI.

Reduce your use of mobile health apps if they are not required. Always consult a doctor about health concerns or changes.

Know that whatever you post online is available for anyone to see. Be selective with what you post.

Try to avoid virtual doctor's visits. Go into the doctor's office when you can.

Using common sense when discussing your health over the internet is also important.



How Open Are You To Sharing Your Data?

After reading this zine, there is one thing you should ask yourself: to what extent am I okay with having my health data used by people other than me? Once you answer this question, you can either continue on how you have been interacting online or begin to implement changes to protect your data better. Some people claim not to care if companies or third parties use their information for unknown purposes, while others are wholeheartedly against it, calling it unethical. It is up to you to decide how or if you want to share your health data with people other than a healthcare provider.



Additional Sources

- *How to protect your online health information*. American Academy of Dermatology. (n.d.). <https://www.aad.org/public/fad/digital-health/protect-information>
 - Take a look at a list of tips from the American Dermatology Association on how to keep personal health data more secure.
- *Legal - Apple Privacy Policy*. Apple. (n.d.). <https://www.apple.com/legal/privacy/en-ww/>
 - Read the privacy policies of companies that produce wearable technology to see exactly how they use your health data.
- *Health Insurance Portability and accountability act of 1996 (HIPAA)*. Centers for Disease Control and Prevention. (n.d.). <https://www.cdc.gov/php/publications/topic/hipaa.html#:~:text=The%20Health%20Insurance%20Portability%20and,the%20patient's%20consent%20or%20knowledge.>
 - Read more about HIPAA. It's important to know how and why your personal health information is protected.
- *The Personal Information Protection and Electronic Documents Act (PIPEDA)*. Office of the Privacy Commissioner of Canada. (n.d.). <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/>
 - Read more about The Personal Information Protection and Electronic Documents Act (PIPEDA), which is said to be Canada's equivalent to HIPAA in the United States.
- *Cherian, S. (2022, January 14). Council post: Healthcare Data: The perfect storm. Forbes.* <https://www.forbes.com/sites/forbestechcouncil/2022/01/14/healthcare-data-the-perfect-storm/?sh=438eb41c6c88>
 - Read this article about the value of health data. Knowing the value of your data is important so you can protect it appropriately.

References

- [1] Houser, S. H., Flite, C. A., & Foster, S. L. (2023). Privacy and Security Risk Factors Related to Telehealth Services - A Systematic Review. *Perspectives in Health Information Management*, 20(1), 1f-10.
- [2] Choudhury, Tanupriya., Katal, Avita., Um, J.-Sup., Rana, Ajay., & Al-Akaidi, Marwan. (2022). *Telemedicine: The Computer Transformation of Healthcare* (1st ed. 2022.). Springer International Publishing. <https://doi.org/10.1007/978-3-030-99457-0>
- [3] Fausett, C. M., Christovich, M. P., Parker, J. M., Baker, J. M., & Keebler, J. R. (2021). Telemedicine Security: Challenges and Solutions. *Proceedings of the International Symposium of Human Factors and Ergonomics in Healthcare*, 10(1), 340-344. <https://doi.org/10.1177/2327857921101241>
- [4] Same as 3.
- [5] Jahankhani, H., Kendzierskyj, S., Jamal, A., Epiphaniou, G., & Al-Khateeb, H. (2019). Cyber-Physical Attacks and the Value of Healthcare Data: Facing an Era of Cyber Extortion and Organised Crime. In *Blockchain and Clinical Trial* (pp. 115-137). Springer International Publishing AG. https://doi.org/10.1007/978-3-030-11289-9_5
- [6] Same as 5.
- [7] Anguilm, C. (2022, October 27). *How to ensure your telehealth system is HIPAA compliant*. Medical Advantage. [https://www.medicaladvantage.com/blog/ensure-your-telehealth-system-is-hippa-compliant/#:~:text=To%20ensure%20HIPAA%20compliance%2C%20telehealth,business%20associate%20agreement%20\(BAA\)](https://www.medicaladvantage.com/blog/ensure-your-telehealth-system-is-hippa-compliant/#:~:text=To%20ensure%20HIPAA%20compliance%2C%20telehealth,business%20associate%20agreement%20(BAA))
- [8] *Telehealth privacy tips for Providers*. Telehealth.HHS.gov. (n.d.). <https://telehealth.hhs.gov/documents/Telehealth+Privacy+Tips+for+Providers.pdf>
- [9] Glenn, T., & Monteith, S. (2014). Privacy in the Digital World: Medical and Health Data Outside of HIPAA Protections. *Current Psychiatry Reports*, 16(11), 494-494.
- [10] Same as 9.
- [11] Same as 9.
- [12] Same as 9.
- [13] *Fitbit Privacy Policy*. Google Fitbit. (n.d.). <https://www.fitbit.com/global/en-ca/legal/privacy-policy#how-info-is-shared>
- [14] Vijayan, V., Connolly, J. P., Condell, J., McKelvey, N., & Gardiner, P. (2021). Review of Wearable Devices and Data Collection Considerations for Connected Health. *Sensors (Basel, Switzerland)*, 21(16). <https://doi.org/10.3390/s21165589>

CONFIDENTIAL

How to cite this zine:

Sheppard, Elsie. (2024). Validating or Violating: An Introspective Look on How Health Information is Shared Online. Hamilton.

Created for:

CNMCS 720: Data Cultures. Department of Communication Studies and Media Arts. Winter 2024. Dr. Andrea Zeffiro