IDX™
The Privacy Platform

Digital Privacy in the New Age of Virtual Healthcare

Digital Privacy in the New Age of Virtual Healthcare

Telemedicine provides greater access to healthcare for consumers everywhere, but, as technology progresses, so do the threats to our cybersecurity. Over 93 percent of healthcare organizations have experienced a data breach in the past three years. With data breach and cyber attacks on the rise, healthcare organizations need digital privacy solutions that make telehealth safer for payers, providers, and consumers.

CONTENTS

Modern-Day Threats to Healthcare Consumers

Healthcare organizations have been evolving into the digital space for the past two decades, but progress was slow. Consumers weren't used to attending virtual appointments with doctors, and patients and providers alike hesitated to embrace unfamiliar technologies. All this changed in 2020 when the pandemic hit, and the world shifted to a different mode of operation. Suddenly, telemedicine was the go-to method for interacting with patients, and care providers rapidly developed innovative ways to scale their remote capabilities.

The changes brought on by COVID-19 are here to stay. 57 percent of healthcare providers view telehealth more favorably than they did before COVID-19, and 64 percent are more comfortable using it, according to a recent report on telehealth by McKinsey & Co.[1] Patients are also reporting higher levels of satisfaction with their virtual health experiences. The types of digital services are expanding too, with up to $250 billion of current US healthcare spend expected to be virtualized in the near future.

57% of healthcare providers view telehealth more favorably than they did before COVID-19

64% are more comfortable using it

93%

of healthcare consumers said they would leave their provider if an attack that could have been prevented compromises their data.

Unfortunately, with all the benefits of telemedicine comes risk. Risks to our digital privacy. Risks to our medical identities. Risks to sensitive patient data. The frequency of cyberattacks on healthcare organizations is exploding while 73 percent of healthcare providers[2] report that their infrastructures are unprepared to respond. Still, customers want and expect more options for virtual care and all the advantages that come with digitized capabilities. They will choose to work with the providers who can give them better options while protecting their patient privacy.

In a recent poll[3], 93 percent of healthcare consumers said they would leave their provider if an attack that could have been prevented compromises their data. Going forward, the industry's challenge will be investing in the tools that secure our health systems while embracing growing virtual options.

[1] https://www.mckinsey.com/industries/healthcare-systems-and-services/our-insights/telehealth-a-quarter-trillion-dollar-post-covid-19-reality
[2] https://www.prnewswire.com/news-releases/attacks-predicted-to-triple-in-2021-black-book-state-of-the-healthcare-industry-cybersecurity-industry-report-301172525.html
[3] https://www.prnewswire.com/news-releases/attacks-predicted-to-triple-in-2021-black-book-state-of-the-healthcare-industry-cybersecurity-industry-report-301172525.html

Apps, Connected Devices, and AI, Oh My!

Part of the role healthcare companies play in protecting customers from bad actors lies in educating them about threats to their digital privacy. There are risks in new technologies, of which most consumers remain largely unaware. When healthcare patients fall for a scam, it could create vulnerabilities in connected health systems, potentially affecting the security of other patients' data.

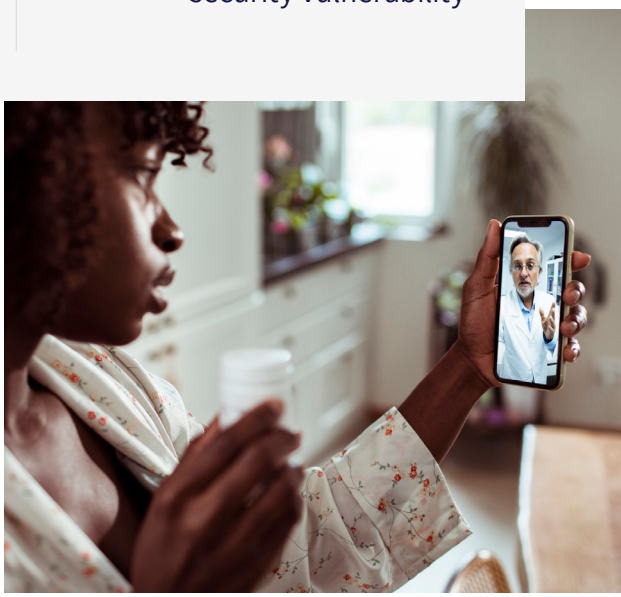
Tools like mobile telehealth applications, connected devices, and artificial intelligence are already negatively impacting digital privacy. Hackers have had the advantage as consumers ramp up adoption of the latest and greatest while providers are still rushing to invest in cybersecurity solutions that can keep up with a rapidly evolving threat landscape.

Consumer usage of mobile health tracking apps was already on an upswing before the pandemic. COVID-19 fast-tracked the rise of these medical applications when health agencies began using contact tracing apps to assist with symptom tracking and exposure notifications. Unfortunately, security investigations have revealed[4] that 85 percent of COVID tracking apps leak data, 91 percent have weak encryption, and 71 percent contain at least one security vulnerability.

85% of COVID tracking apps leak data

91% have weak encryption

71% contain at least one security vulnerability



Consumer telehealth apps may even be selling the sensitive medical data they collect to other entities for marketing and advertising purposes. Third-party apps do not fall under the Health Insurance Portability and Accountability Act (HIPPA) and aren't subject to federal regulations as long as they are only making claims around general wellness.

So, where does this leave businesses and consumers who want to utilize them? After all, these apps enable better patient-to-provider communications and a wealth of medical data that could help doctors deliver better care to their patients. The trick will be implementing full-scale digital privacy solutions that allow providers to be proactive in their engagement with users while giving control over their data back to consumers. Things like ad and tracking blocking software and encrypted virtual private networks will help consumers protect themselves and feel equipped to stay safe online.

[4] https://www.intertrust.com/resources/healthcare-app-security-report-2020/

The High Stakes of Unguarded, Connected Medical Devices

Remote connection to medical devices has unlocked incredible advancements in patient care. Wearable technologies like heart rate sensors and oximeters give doctors deeper insights into patient health over time. These devices help assess health risks in real-time, allowing doctors to intervene with appropriate care before users face serious issues or a decline in their health. Internal medical hardware with remote connection capabilities like insulin pumps and pacemakers facilitate at-home monitoring and frequent check-ins without requiring in-clinic visits.

The downside to the Internet of Things (IoT) progressing into the medical space is that these technologies are rarely secure. Wireless antennas transmit vital, sometimes life saving data from implanted devices to doctors for assessment, but the data is not encrypted and the devices can be hacked[5]. The FDA is working on addressing these cybersecurity concerns, but healthcare entities must do their part to build back consumer trust and confidence in these tools. Encourage, for example, the regular use of tools like ForgetMe Data Removal to continuously scan and clear away personal data from data broker sites or CyberScan Dark Web Monitoring to help patients proactively monitor the web for their private information.

Artificial Intelligence's (AI) Role in Compromised Medical Platforms

Big data. Artificial intelligence. Digitalization is shaping new ways to use the information in patient records to improve patient care and optimize health services. From diagnosing breast cancer in mammograms[6] to maximizing operating room efficiencies[7], AI's potential for supporting healthcare professionals feels limitless. But we know that these data-driven breakthroughs have created the potential for significant risks. Without more robust cybersecurity solutions to complement these innovations, we're leaving our data and systems open to attack.

AI technology can be particularly tricky to protect. To make the biggest difference, AI needs to be able to access multiple systems and analyze an enormous amount of data. AI algorithms connect to different platforms to access extensive data pipelines. If one connection point is breached, the entire system could be compromised.

Mobile health tracking applications, connected medical devices, and artificial intelligence will play an important role in the new age of virtual healthcare. Advancements in these technologies will continue to enhance care for patients and help healthcare professionals serve their patients in new ways. But, to use these tools, we can't forget the risk side of the equation. To truly benefit from all the innovations telemedicine has to offer, healthcare organizations need to take the initiative to establish plans, practices, and tools that bolster patient privacy and digital security.

[5] https://cybersecurityventures.com/patient-insecurity-explosion-of-the-internet-of-medical-things/
[6] https://www.theguardian.com/society/2020/jan/01/ai-system-outperforms-experts-in-spotting-breast-cancer
[7] https://link.springer.com/article/10.1007/s10729-018-9457-3

The Costs of Unprotected Healthcare Resources

Even though customers have demonstrated an interest in telehealth solutions, something is preventing them from fully adopting these time-saving, money-saving, and in some cases, life-saving tools. It's not hard to see why.

More than 93 percent of healthcare organizations have experienced a data breach since Q3 2016 and 57 percent have had more than five data breaches during the same timeframe.

In 2020, hackers took advantage of the crisis to escalate their activity and broaden their reach, targeting health systems and medical devices. In an interview with Healthcare Finance News,[9] CEO and co-founder of IoT cybersecurity firm Sternum, Natali Tshuva, said, "Hackers know that the healthcare industry is a mess right now in terms of cybersecurity and this gives them even more motivation to create more and more attacks."

More than **93%** of healthcare organizations[8] have experienced a data breach since Q3 2016

57% have had more than five data breaches during the same timeframe

Eroding consumer confidence in online and virtual resources results in gaps in care. When patients are afraid of exposing their health data in a digital environment, treatment compliance crumbles and positive health outcomes wane. Healthcare entities need to build trust and confidence in their ecosystem of care providers to impart the best level of support for their members. Customer satisfaction also suffers in the wake of decreasing care utilization and management. How can we embrace the new age of virtual healthcare while increasing customer engagement in a timely, personalized way?

The answer lies in investing in the right tools and infrastructure to give users back control over their own digital privacy. When your customers are empowered to protect their privacy, they will feel more confident in your care, leading to better care management and customer engagement. Not only do you gain happier, healthier customers, but putting digital privacy tools in the hands of your employees and members also helps to mitigate risks to your health systems at large from unsecured third-party platforms and risky consumer activities.

The costs to healthcare organizations don't end with diminishing consumer confidence. A 2020 IBM report[10] on data breaches found that healthcare companies incur the highest average breach costs out of the industries studied at $7.13 million. This is a 10% increase compared to the 2019 study. With threats four times as likely[11] to center on healthcare than any other industry and ransomware attacks rising rapidly,[12] taking a proactive approach to reduce cyber threats and secure patients' digital privacy is the only way forward.

[8] https://blackbookmarketresearch.newswire.com/news/healthcare-data-breaches-costs-industry-4-billion-by-years-end-2020-21027640
[9] https://www.healthcarefinancenews.com/news/number-cybersecurity-attacks-increase-during-covid-19-crisis
[10] https://newsroom.ibm.com/2020-07-29-IBM-Report-Compromised-Employee-Accounts-Led-to-Most-Expensive-Data-Breaches-Over-Past-Year
[11] https://www.prnewswire.com/news-releases/attacks-predicted-to-triple-in-2021-black-book-state-of-the-healthcare-industry-cybersecurity-industry-report-301172525.html
[12] https://newsroom.ibm.com/2021-02-24-IBM-Security-Report-Attacks-on-Industries-Supporting-COVID-19-Response-Efforts-Double

IDX
The Privacy Platform

Forward-Thinking Solutions for an Uncertain Digital Age

Consumers need to be able to trust that their healthcare providers are looking out for them. Making investments in new technologies that will help you optimize patient resources and save you money won't mean anything if your customers aren't willing to engage with them. Healthcare organizations big and small are at a crossroads when it comes to cybersecurity and digital privacy. The industry will either invest in the future or continue to fall prey to cyber attacks, losing millions of dollars and their customers' trust in the process.

Privacy is Proactive

Keep ahead-of-the-curve and safeguard your customers' trust with an all-in-one security platform designed to empower your members and employees with privacy and identity protection for a modern, digital landscape. As a leader in privacy and identity solutions, IDX has built a consumer-centered, easy-to-use platform to equip consumers with everything they need to help minimize risks to their digital privacy. Drive better customer engagement with the industry's leading privacy engagement platform. Contact a healthcare solutions representative today.

Learn more about protecting your employee, members, and ultimately your company from cyber threats with IDX award-wining identity and privacy solutions.

www.idx.us/enterprise-solutions