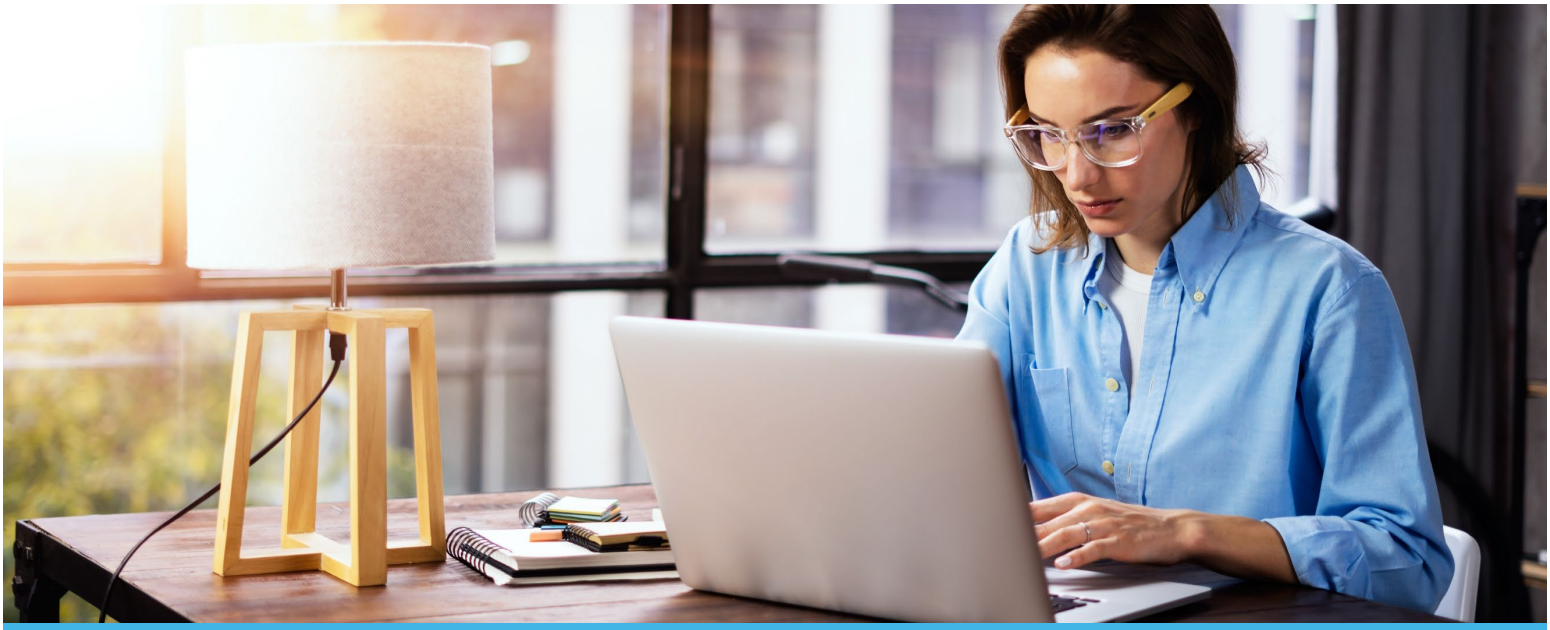


DIGITAL HEALTHCARE TOOLS & DATA SECURITY: ARE CONSUMERS CONCERNED?

BY: JEREMY COCHRAN & ALEX MANGOFF

Digital healthcare tools are becoming more popular, with over half of Americans using one. Consumers are expecting healthcare to have a digital component, and providers and payers are getting in the game. But these apps store a great deal of personal information about consumers that could be exposed in a security breach. Are consumers worried? In general, no; they see healthcare digital tools as secure as other online tools such as those for online shopping and banking. Yet if security breaches become more common, consumers may lose trust and opt-out of volunteering their information. Healthcare companies looking to create or expand their digital tools should continuously invest in data security, communicate their security priorities to consumers, and create clear and simple privacy policies.

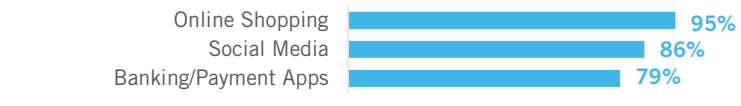
The digital healthcare market is big and getting bigger. In our current COVID-19, socially-distancing environment, digital services such as telemedicine can play a crucial role in providing access to health care and health care providers. According to recent Burke internal research, over half of Americans have used some sort of healthcare-related tool. These tools can include consumer-focused aids such as fitness trackers, healthy eating apps, and medication organizers, as well as more provider-focused tools such as patient portals, remote patient monitoring, and telemedicine video apps.[1] The popularity of these tools is resulting in an increase in the digital health market: the market for mobile health care apps was $5 billion in 2019 and is projected to reach $50 billion by 2025.[2] While most of the interest in digital healthcare tools comes from consumers, providers are also going digital with increased use of patient portals, remote patient monitoring, and telemedicine.

Not only are consumers embracing healthcare technology, they are increasingly expecting it from their healthcare providers. In a recent survey by Accenture, consumers said they would be more likely to choose a provider that offered digital reminders for follow-up care (70%), can communicate with patients through secure email (69%), use remote health tracking/monitoring (53%), and offer video conferencing consultation (49%). These expectations are especially true for younger consumers (Gen X, Millennials, and Gen Z).[3] Providers are adapting; around 90% of healthcare organizations use patient portals, with just under half of them accepting patient-generated health data.[4]

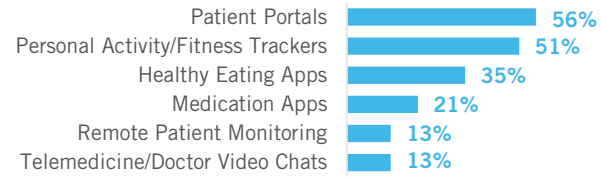
Payers and insurers are also noticing the increased interest in digital healthcare and are moving to take advantage: Aetna and CVS have recently partnered with Apple to create a new app that integrates consumers' personal health activity (e.g. exercise, heart rate, steps) with their health history to create individual improvement plans.[5] UnitedHealthcare has Navigate4Me, a program that collects health tracking data from digital devices for Medicare Advantage participants; Navigator representatives use that data to identify future health actions and anticipate long-term needs.[6]

Burke
SINCE 1931

USE OF NON-HEALTHCARE RELATED DIGITAL TOOLS



USE OF HEALTHCARE RELATED DIGITAL TOOLS



HEALTHCARE INFORMATION, PRIVACY, AND SECURITY

The increase in personal health tracking, along with the digitizing of health records, has created an increase in the amount of consumer health data available, prompting concerns about data security and privacy. While federal regulations, such as the Health Insurance Portability and Accountability Act (HIPPA), exist to help protect individuals' health records, applying them to consumer-focused health tools can be difficult.

Data security could be concerning given the amount and type of data collected. Fitness apps like Fitbit store your steps and exercise habits, of course, but also more detailed information like heart rate, location, sleep patterns, and weight (not to mention credit card information). More specific apps can store even more personal information like menstrual cycles, sexual behavior, and medication history. If this data were to be breached, users' financial data, location, and personal health information could be exposed and possibly used against them.[7]

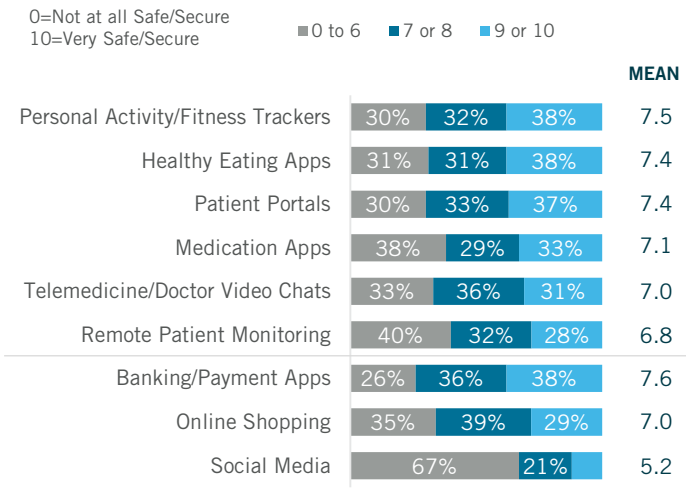
Some of these apps have been hacked already. In 2018, MyFitnessPal reported a security breach that exposed usernames and passwords for 150 million users[8]; in 2016, a small number of Fitbit users had their accounts hacked and their login information and location data exposed.[9] While the fallout from these security breaches has been relatively limited, the large number of users and data stored in these tools creates the potential for more damage.

CONSUMERS GENERALLY UNCONCERNED ABOUT PRIVACY IN HEALTHCARE TOOLS

How much do concerns about data security impact consumers' use of health technology? Given the tech's increasing popularity, it does not seem to hold them back. Why? Recent internal research by Burke may help give the answer: consumers were asked for their perceptions of how secure their data was on various healthcare and non-healthcare digital tools. Banking/payment apps were rated as most secure, followed by online shopping platforms; social media was considered much less secure.

Consumers felt that the healthcare tools, which included both consumer tools (fitness trackers, nutrition apps, medication reminder tools) and provider-focused tools (patient portals, telemedicine, remote monitoring), were at least as secure as online shopping platforms and much more secure than social media apps. Interestingly, the consumer-focused tools, which are generally not linked to a healthcare provider and thus fall farther from federal regulations, were considered more secure than provider-focused ones.

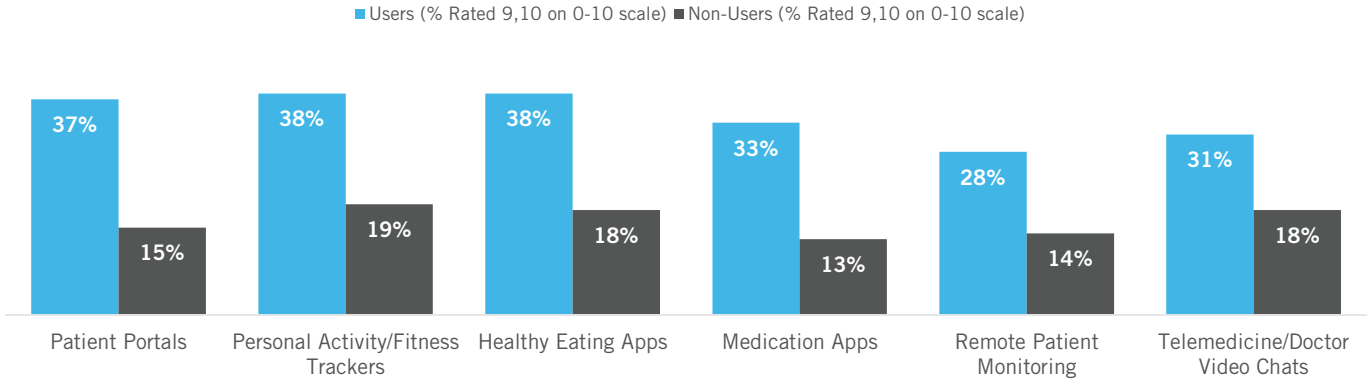
PERCEPTIONS OF SECURITY OF HEALTHCARE-RELATED DIGITAL TOOLS WITH REGARD TO PERSONAL HEALTH INFORMATION AMONG USERS:



DIGITAL HEALTHCARE TOOLS & DATA SECURITY: ARE CONSUMERS CONCERNED?

The Burke data also showed that privacy concerns are much lower for consumers who have actually used the tool compared to those who have not. Around two-in-five consumers who have used a tool feel that it is very secure, compared with only one-in-five for those not using it. Consumers who are more interested in using the app may be more willing to take on any potential security risks, and vice versa.

PERCEPTIONS OF SECURITY OF DIGITAL TOOLS WITH REGARD TO PERSONAL HEALTH INFORMATION (PHI):



Furthermore, when looking at the how well specific brands ensure data privacy, FitBit was rated similar to that of Google (interestingly, both are now part of the same company). Consumers appear to trust that tech companies overall are keeping their data safe, and see their health information in the same way.[10]

PERCEPTIONS OF HOW WELL BRAND ENSURES PRIVACY OF PERSONAL INFORMATION...

amazon — **8.2** out of 10, **53%** rate 9 or 10

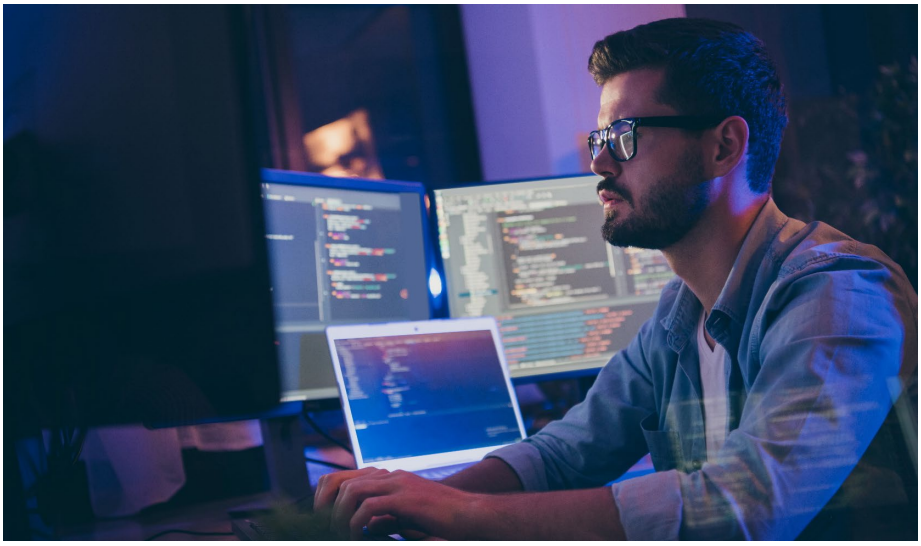
PayPal — **8.1** out of 10, **53%** rate 9 or 10

fitbit — **7.5** out of 10, **39%** rate 9 or 10

Google — **7.3** out of 10, **33%** rate 9 or 10

FACEBOOK — **6.1** out of 10, **19%** rate 9 or 10

CONCLUSION



In general, security concerns are not a primary issue for consumers when considering using a digital healthcare tool. Most consumers currently trust the tools to keep their data safe, or at least feel that their data is as safe as other non-healthcare data.

However, more security breaches are likely to occur. If these breaches become more widespread or expose more personal information, consumers may become more wary of using these tools and demand more upfront assurances on data security.

MOST CONSUMERS CURRENTLY TRUST THE TECHNOLOGY COMPANIES BEHIND THEIR TOOLS TO KEEP THEIR DATA SAFE, OR AT LEAST ASSUME THAT THEIR DATA IS AS SAFE AS OTHER NON-HEALTHCARE DATA.

Healthcare organizations using or developing these tools can get ahead of the curve by:

- **Continually improving data security** – the best way to ensure that one's brand is not associated with security problems is to not have a security problem. Yet threats to data security are always evolving, so protection against these threats must always be improving Continually Investing in data security to ensure the safety of consumer data should be the top priority.
- **Develop communications to prove to consumers that their data are safe** – At present, consumers generally trust that their data is safe, even if they don't necessarily know how. But security breaches will happen in the future, potentially eroding this trust. If consumers become more suspicious of whether healthcare apps are protecting their data, they may gravitate towards brand that can demonstrate that security is a clear priority for them.
- **Be open and transparent about how members' data are used** – In addition to knowing their data are safe, consumers should know exactly how their data are being used and why. Develop clear and simple privacy policies that show consumers where their data ends up, and give them the power to control how their data is used.

ABOUT THE AUTHORS

JEREMY COCHRAN, PsyD
SR. CONSULTANT, DECISION SCIENCES

Jeremy sees his role as simple: answer his clients' questions, both spoken and unspoken. As a psychologist and market researcher, Jeremy is passionate about finding out why people do what they do.

CONTACT: JEREMY.COCHRAN@BURKE.COM

ALEX MANGOFF
SR. CONSULTANT, DECISION SCIENCES

With over a decade of experience, Alex is enthusiastic about leveraging research to provide clients with actionable insights and clear direction on how to grow their brands and business.

CONTACT: ALEX.MANGOFF@BURKE.COM

SOURCES:

[1] Burke, Inc. (2019). *Insights into Key Healthcare Topics.* Burke, Inc.

[2] Grand View Research. (2019). *Mobile health apps market forecast in the United States from 2018 to 2025, by type (in million U.S. dollars).* In Statista – The Statistics Portal. Retrieved December 13, 2019.

[3] Safavi, K., Webb, K., & Kalis, B. (2019). *Accenture 2019 Digital health Consumer Survey.* Accenture. https://www.accenture.com/_acnmedia/pdf-94/accenture-2019-digital-health-consumer-survey.pdf

[4] Medical Group Management Association. (2018, July 26). *MGMA Stat: Most practices offer a patient portal.* https://www.mgma.com/news-insights/quality-patient-experience/mgma-stat-most-practices-offer-a-patient-portal

[5] Landi, H. (2019, January 30). *Aetna launching new Apple Watch app to gather health data, reward healthy behavior.* FierceHealthcare. https://www.fiercehealthcare.com/tech/aetna-launching-new-apple-watch-app-to-gather-health-data-reward-healthy-behavior

[6] Renfrow, J. (2019, February 20). *UnitedHealthcare expands digital data collection for Medicare beneficiaries.* FierceHealthcare. https://www.fiercehealthcare.com/payer/unitedhealthcare-expands-digital-data-collection-for-medicare-participants

[7] Koch, R. (2019, October 31). *Fitness apps are good for your health, but often bad for your privacy.* Security Boulevard. https://securityboulevard.com/2019/10/fitness-apps-are-good-for-your-health-but-often-bad-for-your-privacy/

[8] Germano, S. & Armental, M. (2018, March 29). Under Armour Discloses Breach Affecting 150 Million MyFitnessPal App Users. *The Wall Street Journal.* https://www.wsj.com/articles/under-armour-discloses-breach-affecting-150-million-myfitnesspal-app-users-1522362412

[9] Spary, S. (2016, January 6). *Online Criminals Are Targeting Fitbit User Accounts.* BuzzFeed News. https://www.buzzfeednews.com/article/saraspary/online-criminals-are-targeting-fitbit-user-accounts

[10] Burke, Inc. (2019). *Insights into Key Healthcare Topics.* Burke, Inc.