

# Mobile Telehealth Becomes Critical During the Pandemic

But recent security woes illustrate the security and privacy risk of health and wellness apps.



Telehealth visits skyrocketed during the height of COVID-19 with virtual primary care visits growing from about 2,000 per week in February to roughly 1.28 million per week in mid-April, according to the U.S. Department of Health and Human Services.<sup>1</sup> Accelerated by COVID-19, the mobile health and wellness market is forecast to climb an astounding CAGR 37.3% in North America through 2025.<sup>2</sup> Other major factors driving growth include the rising number of smartphone and tablet users and innovative telehealth apps.



Growth of mental health mobile app sessions in 2020<sup>3</sup>

Mobile telehealth apps encompass everything from telemedicine such as Doximity and Medici; personal medical records such as MyChart and My Medical; pharmacies such as GoodRx and Rite Aid; health and wellness such as Calm and Headspace; fitness such as Peloton and SWEAT; and Internet of Things (IoT) apps such as Fitbit and DreamMapper.

## Mobile Apps Improve Healthcare Access

With much of the population homebound, people rely on mobile apps to consult with doctors, monitor symptoms, fill prescriptions and find exercise and meditation routines. Health and fitness apps surged 30% from Q1 to Q2 2020, while medical apps grew 20%.<sup>4</sup> Indeed, eMarketer forecast the number of

U.S. smartphone users of health and fitness apps increased 27.2% in 2020 to reach 87.4 million.<sup>5</sup>

The Mayo Clinic has been investing in mobile health apps for years and now has more than one million users of its mHealth app.<sup>6</sup> The clinic is exploring use of emerging technologies such as artificial intelligence, connected health devices and natural language processing to accelerate research and improve outcomes. In addition, it partnered with Safe Health Group to develop a health passport app with an initial focus on COVID-19. The goal is to provide real-time health status information such as a negative COVID test or vaccine while also protecting consumer privacy.<sup>7</sup>

## Mobile App Breaches Spotlight Industry Concerns

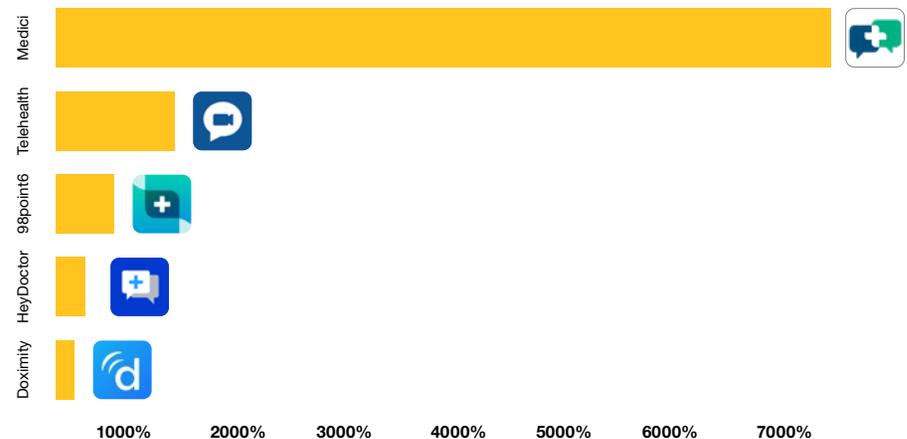
As demand for healthtech apps continues to climb, so does the threat landscape that puts sensitive patient data at risk. IoT apps connected to medical devices to measure heart rate, blood pressure and levels of sugar collect an abundance of personal medical information.<sup>8</sup> Hacking them

could even lead to a deadly scenario if attackers were to take control of a pacemaker or insulin pump.<sup>9</sup>

A recent study of healthcare and medical mobile apps by Intertrust underscored the danger.<sup>10</sup> Alarmingly, 91% of apps have mishandled and/or weak encryption that puts them at risk for data leakage and intellectual property theft. 85% of COVID-tracking apps leak data. 71% have at least one high-level vulnerability that could

## Mobile Telehealth App Engagement Soars

Social distancing sparked sky-high engagement rates for telehealth apps. The chart below shows year-over-year percentage gains for daily active users of the fastest growing telehealth apps in April 2020.<sup>11</sup>



## Compromising an IoT medical app could potentially lead to a life-or-death scenario.

lead to a breach of medical data. And 34% of Android apps and 28% of iOS apps are vulnerable to encryption key extraction.

Several telehealth apps were recently revealed to have risky vulnerabilities, privacy flaws and compliance issues. Consider these incidents:

- A **Babylon Health** mobile app security vulnerability allowed patients to view recordings of others' video consultations with doctors. One user claimed he had access to more than 50 video recordings from the leading telehealth provider.<sup>12</sup>
- Smartwatch maker **Garmin** suffered a ransomware attack that took down its Garmin Connect and Garmin Golf apps for several days.<sup>13</sup> Garmin reportedly paid a \$10 million ransom to a Russian hacking group.<sup>14</sup>

- Pharmacy giant **Walgreens** warned that a security error in its messaging app potentially exposed customer names, prescriptions and shipping addresses.<sup>15</sup>
- Medical device manufacturer **Philips** issued an advisory and the Department of Homeland Security issued an alert about an encryption vulnerability affecting versions of the Philips HealthSuite Health Android app.<sup>16</sup>
- An **Under Armour** data breach leaked sensitive information of roughly 150 million MyFitnessPal app users.<sup>17</sup>
- The popular **Strava** fitness tracking app revealed sensitive locations of U.S. troops by publishing geolocation activity of jogging routes around war zones and military facilities around the globe.<sup>18</sup>

Such security incidents demonstrate the need for deep mobile application security testing to uncover security vulnerabilities, privacy flaws and maintain compliance with strict healthcare regulations such as HIPAA.

Automated mobile application security testing tools enable AppDev, AppSec and DevSecOps teams to test apps on demand or perform continuous security

testing directly in the development pipeline. The NowSecure solution performs deep testing to clearly identify risks of Android and iOS mobile apps so companies can address them before releasing those apps to the public. In addition, the company's expert penetration testing services can give organizations peace of mind that their sensitive apps are secure.

### About NowSecure

NowSecure offers a comprehensive suite of automated mobile appsec testing solutions, penetration testing and training services to reduce risk. Trusted by many of the world's most demanding organizations, NowSecure protects millions of app users across banking, insurance, high tech, retail, healthcare, government, et al. The company is SOC2 certified and was recently named a mobile security testing leader by IDC, a DevSecOps transformational leader by Gartner, and a Deloitte Technology Fast 500 winner.

**71%**  
of healthcare and medical apps have at least one serious vulnerability<sup>10</sup>

Visit [www.nowsecure.com](http://www.nowsecure.com) to discuss strategies for strengthening the security of mobile telehealth apps to safeguard personal information and maintain compliance.

### SOURCES

- <sup>1</sup> Assistant Secretary for Planning and Evaluation, "[Medicare Beneficiary Use of Telehealth Visits: Early Data from the Start of the COVID-19 Pandemic.](#)" July 28, 2020
- <sup>2</sup> Fractovia, "[4 Prominent Trends Shaping the North American Digital Health Market Through 2025.](#)" Nov. 17, 2020
- <sup>3</sup> Apptopia, "[Calm Records 120% More App Sessions Than Headspace During Quarantine.](#)" June 16, 2020
- <sup>4</sup> App Annie, "[Mobile App Usage Surged 40% During the Pandemic.](#)" July 8, 2020
- <sup>5</sup> eMarketer, "[The Number of Health and Fitness App Users Increased 27% from Last Year.](#)" July 20, 2020
- <sup>6</sup> Mhealthintelligence.com, "[Telehealth Helps the Mayo Clinic Adjust to a New Healthcare Ecosystem.](#)" Nov. 16, 2020
- <sup>7</sup> FierceHealthcare.com, "[Mayo Clinic, Startup Launch 'Health Passport' App with Initial Focus on COVID-19.](#)" Oct. 12, 2020
- <sup>8</sup> TechieExpert, "[Telemedicine App Development Benefits and Types.](#)" Oct. 22, 2020
- <sup>9</sup> Wired, "[Hackers Made an App That Kills to Prove a Point.](#)" July 16, 2020
- <sup>10</sup> Help Net Security, "[85% of COVID-19 Tracking Apps Leak Data.](#)" Sept. 30, 2020
- <sup>11</sup> Apptopia, "[Telehealth Apps See Highest Engagement In History: MyChart Leads with Most Users.](#)" May 29, 2020
- <sup>12</sup> The Verge, "[Telehealth App Babylon Health Allowed Users to View Other Patients' Video Consultations.](#)" June 10, 2020
- <sup>13</sup> ZDNet, "[Garmin's Outage, Ransomware Attack Response Lacking as Earnings Loom.](#)" July 27, 2020
- <sup>14</sup> Cyber Security Hub, "[Incident of the Week: Garmin Pays \\$10 Million to Ransomware Hackers Who Rendered Systems Useless.](#)" Aug. 14, 2020
- <sup>15</sup> Threatpost, "[Walgreens Mobile App Leaks Prescription Data.](#)" March 2, 2020
- <sup>16</sup> Careers Info Security, "[Weak Encryption Leaves Mobile Health App at Risk for Hacking.](#)" Dec. 11, 2018
- <sup>17</sup> CNBC, "[Under Armour Says Data Breach Affected About 150 Million MyFitnessPal Accounts.](#)" Marcy 29, 2018
- <sup>18</sup> NowSecure, "[U.S. Soldiers and Athletes Using Strava Social Fitness Apps: Finding Risky Mobile Apps That Share and Leak Data.](#)" Jan. 30, 2018