MAR 12

Erum Ahmed

Healthcare APIs will become big hacker targets in 2022, but Google Cloud could have a solution

Article

The news: Google Cloud is making its **Healthcare Consent Management API** generally available to customers: Early adopters have already used the API to build personalized patient portals, securely integrate data into clinical workflows, and create virtual clinical trials, according to Google.

Here's how it works: Google Cloud's API ensures providers and researchers are meeting privacy requirements and getting patients' consent before accessing their health data through devices like wearables or glucose monitors.

For example, patients may opt to partake in clinical research or use telehealth from home, but they'll still want control over how and by whom their data is accessed. Google's Content Management API will serve as a checkpoint for healthcare developers leveraging patient data: If a researcher wanted to access a patient's wearable data to obtain their past blood pressure readings, for instance, they'd have to send a query to Google's Healthcare Consent Management API, which rapidly decides whether there's a "valid consent record permitting that access."

How we got here: Google Cloud's new API diversifies its portfolio of healthcare cloud offerings, which have already nabbed the attention of players from every corner of the digital health ecosystem.

- **Health insurance companies:** In December, healthcare delivery network **Highmark Health** signed a six-year contract with Google Cloud to enhance coordination among the care teams it works with—indicating cloud investments are a long-term priority for payers as the **HHS'** mandates force insurers to put interoperability on the top of their priority list.
- **Telehealth vendors:** Last August, Google Cloud inked a **$100 million** deal with **Amwell** to seamlessly host virtual care visits while boosting the telehealth company's interoperability with hospitals. This move arrives as large health systems are tying up with cloud giants to improve data sharing beyond hospital walls: Large health system **Providence** uses **Microsoft Cloud** to boost easier access and exchange of electronic health record data between healthcare providers and health plans, for instance.

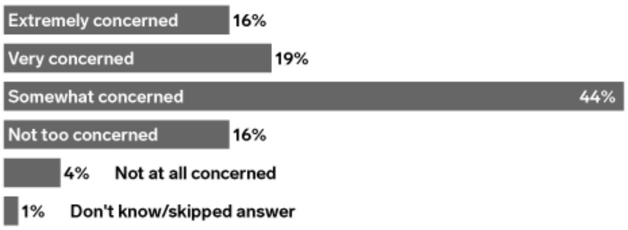
Why this could succeed: Analysts predict mobile health apps will increasingly leak sensitive data through APIs, so solutions like the Consent Management API will be in high demand.

- Most mobile health apps are susceptible to API attacks enabling bad actors to access patients' EHR information. For example, researchers tested 30 mobile health apps and found they collectively exposed **23 million** users to data breaches—and unauthorized medical professionals were able to access pathology and lab results of other patients in 50% of tested APIs, according to a recent report by mobile security company Approov.

- However, Google Cloud's New Consent Management API stops unauthorized individuals from accessing patient data to some extent: The new consent tool allows providers and researchers to only get their hands on the specific data a patient has consented to sharing.
- By 2022, API attacks will become the most frequent channel for app breaches, according to Gartner. So, developers will have to assure patients that their data is protected if they want to see higher consumer adoption of their particular app or wearable.

Level of Concern that US Adults Have About the Privacy of Their Medical Information and Data*, July 2020

% of respondents



*Note: *if they download it to different health apps they have selected to use on their smartphone, computer, or table*
Source: The Pew Charitable Trusts, "Pew HIT National Survey" conducted by Public Opinion Strategies and Hart Research Associates, Sep 16, 2020

258920 eMarketer | InsiderIntelligence.com