

# Amazon, One Medical, and BetterHelp targeted by the FTC

## Article

**The trend:** The Federal Trade Commission (FTC) is investigating how digital health companies are protecting health data. It's targeting advertising practices with social media platforms—but also looking for any **inferred or explicit promises to keep that data private.**

**How we got here:**

- In February, the [FTC fined GoodRx \\$1.5 million](#) for sharing users' personal health data with social media platforms like Facebook and Google. FTC commissioners also issued a joint statement on **Amazon's acquisition of One Medical** that warned the entities against using patient health data for advertising purposes, despite explicit statements to consumers that wouldn't happen.
- In early March, **Teladoc-owned BetterHelp** was hit with a **\$7.8 million fine** based on data sharing with social media platforms for advertising purposes—and for statements that the patient's data would remain private between the patient and an assigned counselor.

**Why it matters:** The FTC doesn't have jurisdiction over HIPAA violations. It enforces Section 5 of the FTC Act, which prohibits “deceptive acts or practices . . . relating to the privacy and security of personal information that apps collect, use, maintain, or share.”

### **Marketers are often untrained in regulations surrounding sensitive healthcare data.**

BetterHelp was cited for giving a junior marketing analyst carte blanche to decide which data to upload to Facebook and how to use that information. The person joined BetterHelp in 2017, but didn't receive training on how to protect consumers' health information until 2021, per the FTC.

**The FTC is using consumers—not policy experts—as a gauge to decide if a company is telling the truth about data privacy.** In the notice to Amazon and One Medical, FTC commissioners stated that “whether the companies' privacy representations are deceptive will turn on the perspective of a reasonable consumer rather than the perspective of a HIPAA expert.”

**Our take:** It's what is on the website that matters, not what's buried in an online privacy policy. Digital health companies are justifiably under increasing scrutiny for sharing patients' health data with third parties, without their users' specific consent.

But they're also being held accountable for making statements that any intelligent visitor would understand to mean their data wouldn't be shared anywhere else. That includes promises like “HIPAA-compliant” or “100% confidential.”

## Are Adults in Select Countries Concerned About the Security & Privacy of Their Personal Data?

% of respondents, Sep 2022

	Concerned (net)	Neither concerned/ unconcerned	Unconcerned (net)	Don't know
Spain	84%	8%	7%	1%
Hong Kong	84%	12%	3%	1%
Singapore	83%	10%	4%	2%
India	81%	10%	6%	4%
Indonesia	78%	18%	3%	1%
Australia*	77%	15%	7%	2%
Canada	75%	13%	8%	3%
Great Britain	75%	14%	7%	4%
US	74%	11%	8%	6%
UAE	73%	15%	7%	5%
France	71%	18%	8%	3%
China*	69%	20%	8%	3%
Italy	63%	26%	9%	2%
Poland	62%	22%	11%	5%
Sweden	55%	25%	16%	4%
Germany	53%	27%	15%	5%
Denmark	43%	31%	22%	5%

Note: ages 18+; numbers may not add up to 100% due to rounding; \*ages 16+  
Source: YouGov, "Consumer Electronics: Safety and Sustainability in 2023," Jan 17, 2023

280393

[InsiderIntelligence.com](https://www.insiderintelligence.com)

*This article originally appeared in Insider Intelligence's Digital Health Briefing—a daily recap of top stories reshaping the healthcare industry. Subscribe to have more hard-hitting takeaways delivered to your inbox daily.*

- Are you a client? [Click here to subscribe.](#)
- Want to learn more about how you can benefit from our expert analysis? [Click here.](#)