

Directions:

Read the following four texts. Answer the questions after each text by choosing A, B, C or D. Mark your answers on the **ANSWER SHEET**. (40 points)

Text 4

If you look at the apps on your phone, chances are you have at least one related to your health—and probably several. Whether it is a mental health app, a fitness tracker, a connected health device or something else, many of us are taking advantage of this technology to keep better track of our health in some shape or form. Recent research from the Organization for the Review of Care and Health Applications found that 350,000 health apps were available on the market, 90,000 of which launched in 2020 alone.

While these apps have a great deal to offer, it is not always clear how the personal information we input is collected, safeguarded and shared online. Existing health privacy law, such as the Health Insurance Portability and Accountability Act, is primarily focused on the way hospitals, doctors' offices, clinics and insurance companies store health records online. The health information these apps and health data tracking wearables are collecting typically does not receive the same legal protections.

Without additional protections in place, companies may share (and potentially monetize) personal health information in a way consumers may not have authorized or anticipated. In 2021, Flo Health faced a Federal Trade Commission (FTC) investigation. The FTC alleged in a complaint that "despite express privacy claims, the company took control of users' sensitive fertility data and shared it with third parties." Flo Health and the FTC settled the matter with a Consent Order requiring the company to get app users' express affirmative consent before sharing their health information as well as to instruct the third parties to delete the data they had obtained.

Section 5 of the FTC Act empowers the FTC to initiate enforcement action against unfair or deceptive acts, meaning the FTC can only act after the fact if a company's privacy practices are misleading or cause unjustified consumer harm. While the FTC is doing what it can to ensure apps are keeping their promises to consumers around the handling of their sensitive health information, the rate at which these health apps are hitting the market demonstrates just how immense of a challenge this is.

As to the prospects for federal legislation, commentators suggest that comprehensive federal privacy legislation seems unlikely in the short term. States have begun implementing their own solutions to shore up protections for consumer-generated health data. California has been at the forefront of state privacy efforts with the California Consumer Privacy Act of 2018. Virginia, Colorado and Utah have also recently passed state consumer data privacy legislation.

36. The research findings are cited in Paragraph 1 to show_____.

- [A] the prevalence of health apps
- [B] the public concern over health
- [C] the popularity of smartphones
- [D] the advancement of technology

37. What does the author imply about existing health privacy law?
- [A] Its coverage needs to be extended.
 - [B] Its enforcement needs strengthening.
 - [C] It has discouraged medical misconduct.
 - [D] It has disappointed insurance companies.
38. Before sharing its users' health information, Flo Health is required to_____.
- [A] seek the approval of the FTC
 - [B] find qualified third parties
 - [C] remove irrelevant personal data
 - [D] obtain their explicit permission
39. What challenge is the FTC currently faced with?
- [A] The complexity of health information.
 - [B] The rapid increase in new health apps.
 - [C] The subtle deceptiveness of health apps.
 - [D] The difficulty in assessing consumer harm.
40. It can be learned from the last paragraph that health data protection_____.
- [A] has been embraced by health app developers
 - [B] has been a focus of federal policy-making
 - [C] has encountered opposition in California
 - [D] has gained legislative support in some states