AHIOS Perspective On the Federal Trade Commission's Policy Statement on Health Apps and Connected Devices Issued on September 15, 2021

By Steve Socha, AHIOS member and SVP Central Operations/Provider Solutions at Sharecare

November 9, 2021

The Scope of the new Federal Trade Commission's (FTC) Policy Statement

On September 15, 2021, the FTC issued a policy statement affirming that health apps and connected devices that collect or use consumers' health information must comply with the Health Breach Notification Rule, which requires that they notify consumers and others when their health data is breached.

The Commission noted that health apps, which can track health data such as glucose levels, heart health, fertility and sleep patterns, increasingly collect sensitive and personal data from consumers. The FTC stated that these apps have a responsibility to ensure they secure the data they collect, which includes preventing unauthorized access to such information.

As part of the American Recovery and Reinvestment Act of 2009, Congress included specific provisions to strengthen privacy and security protections for web-based businesses. The law directed the FTC to ensure that companies contact customers in the event of a security breach. Shortly after, the FTC issued the Health Breach Notification Rule, which requires vendors of personal health records and related entities to notify consumers, the FTC, and, in some cases, the media when that data is disclosed or acquired without the consumers' authorization. Over a decade later, health apps and other connected devices that collect personal health data are not only mainstream—and have increased in use during the pandemic—but are targets ripe for scammers and other cyber hacks. Yet, there are still too few privacy protections for these apps.

"While this Rule imposes some measure of accountability on tech firms that abuse our personal information, a more fundamental problem is the commodification of sensitive health information, where companies can use this data to feed behavioral ads or power user analytics," said FTC Chair Lina M. Khan. "Given the growing prevalence of surveillance-based advertising, the Commission should be scrutinizing what data is being collected in the first place and whether particular types of business models create incentives that necessarily place users at risk."

The Rule ensures that entities not covered by the Health Insurance Portability and Accountability Act (HIPAA) face accountability when consumers' sensitive health information is breached. Essentially the FTC said that any health app or connected device company that suffers a breach will be expected to respond in much the same way that a covered entity would if it had a similar breach. This would include notification of affected consumers whose health data was breached. In the statement, the FTC equated PHR vendors and related service providers with health care providers.

This puts those companies that may not currently be subject to HIPAA under similar obligations of securing PHI from hacking or other unauthorized access and holds them accountable to meeting these obligations. Many of these companies have been operating under the impression that since they are not covered entities or business associates under HIPAA that they were not subject to these types of rules.

The result should be that these companies now need to review and/or revamp their security in order to avoid breaches of the information they collect. Companies that fail to comply with the rule could be subject to monetary penalties of up to $43,792 per violation per day.

In order to understand how serious the FTC is about this policy, we will have to watch and see how they react to any breaches from these companies that become public in the coming months. At this point, the policy appears to be enforceable now so the first enforcement could begin at any time.

It is important to note that the FTC is only talking about reacting to breaches rather than putting in place "guard rails" for the use of these APIs. AHIOS feels that this reactive approach is inadequate in protecting consumers and proactive efforts need to be made to ensure security and privacy along the same lines of the Security and Privacy Rules under HIPAA.

How will this policy change the definition of "health care provider" and what are the implications of that?

In the FTC's view, developers of health applications or connected devices are "health care provider[s]" because they "furnish health care services or supplies."

This is a very broad definition of health care provider and will likely be challenged. However, the key issue isn't whether these companies truly provide health care or not, but rather that they have consumers' protected health information (PHI) and they are required to protect it in a similar manner to a health care provider. What isn't clear at this point is whether the use of this information will be put under similar restrictions as it is for those that are subject to HIPAA especially in the area of marketing. AHIOS believes there may be further restrictions on what these companies can do with the data they collect without express permission of the consumer. Hiding it in the fine print is likely not going to be allowed.

What types of apps and connected devices would be covered/impacted by this policy?

The Commission policy statement notes that apps and connected devices such as wearable fitness tracking devices that collect consumers' health information are covered by the Health Breach Notification Rule if they can draw data from multiple sources, and are not covered by a similar rule issued by the Department of Health and Human Services. For example, a health app would be covered under the FTC's rule if it collects health information from a consumer and has the technical capacity to draw information through an API that enables synching with a consumer's fitness tracker.

Right now the major groups of apps would include such things as personal health records (PHRs) and other health tracking apps which can vary from fitness applications to monitoring devices for blood sugar, blood oxygen, etc. The key issue is whether the application or device can draw information from more than one source. That applies to a very large number of apps and devices.

How vulnerable are mobile health apps?

Thirty popular mobile health applications are vulnerable to attacks via their application program interfaces (APIs), according to findings released in a February 2021 report authored by cybersecurity analyst Alissa Knight and published by Approov. The study, All That We Let In, raises concerns that increasing reliance on mobile health apps during the pandemic is drawing threat actors to mobile health applications as their preferred attack surface. The attacks described can permit unauthorized access to full patient records, including protected health information (PHI) and personally identifiable information (PII).

"There will always be vulnerabilities in code so long as humans are writing it," said Alissa Knight, researcher and author of the report. "Humans are fallible. But I didn't expect…all of the APIs to be vulnerable to broken object level authorization vulnerabilities, allowing me to access patient reports, x-rays, pathology reports, and full PHI records in their database. The problem is clearly systemic."

The study examined 30 popular mobile health apps. Each app has been downloaded an average of 772,619 times, and Knight estimates that the 30 apps examined expose at least 23 million mobile health users. The total number of users exposed by the 318,000 mobile health apps now available on major app stores is likely far greater, according to Knight.

I just checked my phone and I have at least 5 apps that would likely fit into this category. I would expect that a large portion of smartphone users have at least one and there are new devices and apps coming out every day. In addition, one of the goals of ONC's Cures Act is to further the use of APIs to access and share health information so the volume is only going to continue to increase.

Is this FTC Policy Statement indicative of a shift in FTC enforcement priorities given the rapid growth of healthcare apps and connected devices?

AHIOS believes it is a shift even though their Health Breach Notification Rule has been around since 2009. The push for simplified flow of health information through APIs and the booming app economy increases the scrutiny on applications that fall outside of HIPAA. Those companies that are under HIPAA are closely regulated and must meet appropriate security and privacy standards. There have been a number of new companies that have sprung up that did not believe they had to protect consumers in

the same way and have been able to cut corners and be more competitive in the market. This new FTC policy statement will likely cause them to reevaluate how they treat consumers' information and require enhanced security measures. This is a good thing for consumers and should help to keep apps with poor security out of the healthcare system.

What advice does AHIOS have for provider organizations as a result of this new FTC policy statement?

AHIOS supports this FTC Policy statement as it protects patients' privacy. If enforced properly, this should help bolster the security of patient information. AHIOS suggests that healthcare providers perform an assessment of any applications and/or trackers that they currently work with or allow to connect in any way with their systems to determine if these companies are properly prepared to deal with compliance issues and ensure that their patients are aware of their rights under this policy.

PHI is a very valuable commodity on the dark web and we are seeing unprecedented breaches in the health care industry due to hacking, phishing, ransomware and other approaches. Despite all the security and training in place, significant numbers of breaches are occurring in this space and fraud is on the rise. All of that is happening in an ecosystem that is already subject to the HIPAA Security and Privacy Rules. It is critical that consumers understand the risks of allowing their protected health information to be utilized by these apps and critically challenge their security before signing on. If not, as one colleague said recently, "At this rate [of breaches], in five more years, PHI will be an antiquated concept."

About the Association of Health Information Outsourcing Services (AHIOS)

Established in 1996, AHIOS is a trade association of leading health information outsourcing companies whose mission is to establish standards of excellence for the Release of Information (ROI) industry. AHIOS strives to achieve the highest levels of patient privacy throughout the ROI process by educating healthcare providers as well as federal and state agencies on the impact of legislative and regulatory initiatives and on the value that specialized ROI software and processes provide in safeguarding patient privacy and lowering healthcare costs. The association has developed a code of ethics, standards and professional values for HIM professionals; established the AHIOS Institute's Certified Release of Information Specialist (CRIS) competency program which tests ROI staff knowledge in protecting the confidentiality of patients' PHI; and continually works to educate the industry on how to remain in compliance with healthcare's complex and ever-increasing regulatory environment. For more information, visit us at www.AHIOS.org and follow us on LinkedIn and Twitter.