Health apps and connected devices that collect or use your patients' health information must comply with federal rules that require a company to notify consumers and others if the health data is breached, according to a recent policy statement from the Federal Trade Commission (FTC).

The AMA applauds the FTC’s guidance that health app developers must comply with the Health Breach Notification Rule. It creates more accountability for data holders by penalizing those who share information without a user’s authorization, which—in addition to constituting a breach of security—could expose the user to discrimination and profiling based on their health data.

The AMA last year responded to the FTC’s request for comment on the rule, urging the commission to expand the Health Breach Notification Rule’s “coverage to specifically include direct-to consumer technologies and services such as mobile health apps, virtual assistants and platforms’ health tools” and to increase enforcement efforts.

In its statement (PDF), the FTC acknowledges that since its initial rule was issued more than a decade ago, there has been an explosion in health apps and connected devices and that the statement serves to “place entities on notice of their ongoing obligation to come clean about breaches.”

The statement clarifies how the rule applies to vendors of personal health records that contain individually identifiable health information created or received by health care providers—which is defined to include a developer of a health app or connected device because it “furnish[es] health care services or supplies.”

It is triggered when these entities experience a “breach of security,” for example, when a health app discloses sensitive health information without users’ authorization. This includes cybersecurity intrusions, nefarious behavior and incidents of unauthorized access. Those who violate the rule can be fined $43,792 per violation, per day. Companies also must contact consumers about the breach
and, in some cases, the media.

**What is covered by the rule?**

The FTC statement says that apps will be covered by the rule if they are able to draw information from multiple sources, such as consumer inputs and application programming interfaces (APIs).

For example, according to the statement, an app falls under the Health Breach Notification Rule if it “collects information directly from consumers and has the technical capacity to draw information through an API that enables syncing with a consumer’s fitness tracker.” Importantly, an app that draws information from multiple sources is covered, even if the health information only comes from one source. For example, a blood-sugar monitoring app that collects the patient’s inputted blood sugar levels and takes non-health information from dates in the phone’s calendar.

FTC officials noted that the rule ensures that entities that the Health Insurance Portability and Accountability (HIPAA) doesn’t cover are held accountable.

“What 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.”

**AMA push for privacy**

The AMA has for years has sought to ensure that as patients’ health information is shared—particularly outside of the health care system—that they have meaningful controls over how their data is being used, with whom it is being shared and that it remains private.

The AMA created a set of privacy principles (PDF), derived primarily from House of Delegates policy, that call for third parties who access an individual’s data to act as responsible stewards of the information, just as physicians promise to maintain patient confidentiality. The principles say individuals should have rights and protections from discrimination and that the responsibility for privacy should rest with data holders beyond just HIPAA-covered entities. They also call for “robust enforcement of penalties” when violations occur.