Digital health data are being created at a dizzying rate yet a significant chunk of that personal information isn't covered by federal privacy and security laws.

Everything from Fitbits to Apple iPhones are logging and storing health-care data that aren't covered under the Health Insurance Portability and Accountability Act.

Digital health-care data pose real privacy risks, and a federal law change to regulate it is likely in the future, Nan Halstead, a health privacy and security attorney with Reed Smith LLP in Washington, told Bloomberg Law in a video interview. Increasing the federal government's privacy and security regulatory scope could force companies like Fitbit to spend more on compliance efforts.

Fitbit sold 2.2 million devices in the first quarter of 2018 and has 25 million active users, while Apple sold 52.2 million iPhones in the second quarter of fiscal year 2018. Fitbit manufactures various fitness tracking devices that collect and store personal health data, and the Apple Health app also collects a variety of consumer-generated health-care data. Apple recently updated its Health app to let consumers access their medical records through their iPhones.

The volume of unregulated health-care data likely exceeds that of regulated data, Halstead said. HIPAA requires health plans and health-care providers to meet certain privacy and security requirements, while nonregulated entities such as Fitbit face no such federal requirements.

A future law will likely focus on consumer protection and could adopt a HIPAA framework, identifying permitted uses and disclosures by companies that hold or collect the data, Halstead said. It's doubtful that HIPAA itself would be expanded to cover the new digital health-care technologies as the law is too ingrained with the claims submission process and wouldn't be a natural fit for the new sector, Halstead said.

Newly created digital health-care data aren't entirely unregulated, Halstead said, noting that state laws cover them.

It's almost certain that the federal government will look to regulate health information that's not subject to HIPAA, Thora Johnson, a health-care attorney with Venable LLP in Baltimore, told Bloomberg Law.

Direct-to-consumer health-care wearables aren't currently subject to HIPAA and are generating enormous volumes of data daily, Johnson said. Wearables include fitness trackers manufactured by Fitbit, Garmin, and other companies.

"If data from these devices and wearables not otherwise subject to HIPAA is altered by an attacker and individuals are harmed, we're likely to see a swift response from the federal level," Johnson said.

That response may include extending HIPAA to all health-care data, regardless of the types of entitles holding the data, Johnson said.

For now, states may continue to issue a patchwork of privacy and security regulations for health-care data.

Lack of Standards

The lack of data privacy and security standards, including health data not protected by HIPAA, is problematic, Iliana Peters, a health-care attorney with Polsinelli PC in Washington, told Bloomberg Law.

While companies not covered by HIPAA may give notice to consumers about how they may use, or even sell, consumer data, such notice may be insufficient, and consumers may not even understand how their data is being used, Peters said. Peters was a former deputy director for the Health and Human Services Office for Civil Rights (OCR).

“Without baseline privacy and security protections for consumers and their data, there are few limits on how companies can use the data,” Peters said.

The Federal Trade Commission requires companies it regulates to have good basic security practices, but that’s limited by the scope of the FTC"s jurisdiction, Peters said.

Without standards to address data security, widespread implementation of security safeguards can’t be verified, leaving consumers and their data vulnerable, Peters said.

It’s likely that HIPAA at some point may be expanded to cover more of the health-care sector, but it’s likelier that Congress and state legislatures will act to implement stronger privacy and security protections for consumer health-care information, Peters said.

Existing Oversight

The Federal Trade Commission has emphasized the sensitivity of consumer-generated health information collected by digital health products, but has said it has adequate authority to regulate the data under Section 5 of the FTC Act, W. Reece Hirsch, a health-care attorney with Morgan, Lewis & Bockius LLP in San Francisco, told Bloomberg Law.

“Right now I don’t anticipate federal legislation or an expansion of HIPAA to regulate consumer-generated health information, particularly after HITECH Act amendments to HIPAA,” Hirsch, a Bloomberg Law advisory board member and former member of an advisory group to the California Office of Privacy Protection, said.

The Health Information Technology for Economic and Clinical Health Act broadened HIPAA privacy and security protections.

However, Hirsch said the Food and Drug Administration is seeking to expand its regulatory authority over medical devices. In April, the FDA rolled out its Medical Device Safety Action Plan, which details cybersecurity risks for devices.

The House Energy and Commerce Committee also is looking at how to secure legacy medical devices common in the health-care industry, Hirsch said.

“Although there are few laws or regulations specifically targeting consumer-generated health information, the digital health space is subject to fairly robust regulation by the FTC, OCR, state attorneys general, and the FDA,” Hirsch said.

To contact the reporter on this story: James Swann in Washington at jswann1@bloomberglaw.com

To contact the editor responsible for this story: Brian Broderick at bbroderick@bloomberglaw.com