General Committee Meeting
Thursday, January 21, 2021
2:30PM – 4:00PM EST

Zoom Link: https://zoom.us/j/95197374326?pwd=SHNqQ09lSUlrNGpjTjUwQXJzZXovQT09
Phone Number: 312-626-6799
Meeting ID: 951 9737 4326
Password: 073789

1. Welcome and Introductions

2. Guest Speaker: HIPAA Coordinated Care Walkthrough
   Diane Sacks, Confidentiality Coalition Counsel

3. 2021 Confidentiality Coalition Priorities

4. Articles of Interest — Attachment 1, 2, 3, 4, 5, 6

UPCOMING MEETINGS:
2/18: Confidentiality Coalition Steering Committee Meeting, 2:00PM – 3:00PM EST
2/18: Confidentiality Coalition General Committee Meeting, 3:00PM – 4:00PM EST

OCR Announces Notification of Enforcement Discretion for Use of Online or Web-Based Scheduling Applications for the Scheduling of COVID-19 Vaccination Appointments

Today, the Office for Civil Rights (OCR) at the U.S Department of Health and Human Services (HHS) announced that it will exercise its enforcement discretion and will not impose penalties for violations of the HIPAA Rules on covered health care providers or their business associates in connection with the good faith use of online or web-based scheduling applications (collectively, "WBSAs") for the scheduling of individual appointments for COVID-19 vaccinations during the COVID-19 nationwide public health emergency. This exercise of enforcement discretion is effective immediately, but has retroactive effect to December 11, 2020.

The Notification explains that the exercise of enforcement discretion applies to covered health care providers and their business associates, including WBSA vendors (as WBSA is defined in the Notification), when the WBSA is used in good faith and only for the limited purpose of scheduling individual appointments for COVID-19 vaccinations during the COVID-19 nationwide public health emergency. Although OCR is exercising enforcement discretion, the Notification encourages the use of reasonable safeguards to protect the privacy and security of individuals' protected health information (PHI), such as using only the minimum necessary PHI, encryption technology, and enabling all available privacy settings.

"OCR is using all available means to support the efficient and safe administration of COVID-19 vaccines to as many people as possible," said March Bell, Acting OCR Director.

The Notification of Enforcement Discretion for Use of Online or Web-Based Scheduling Applications during the COVID-19 Nationwide Public Health Emergency may be found at https://www.hhs.gov/sites/default/files/hipaa-vaccine-ned.pdf *.

Reducing Provider and Patient Burden by Improving Prior Authorization Processes, and Promoting Patients' Electronic Access to Health Information CMS-9123-F: Fact Sheet

Jan 15, 2021

This final rule places new requirements on Medicaid and CHIP managed care plans, state Medicaid and CHIP fee-for-service programs, and issuers of individual market medical Qualified Health Plan (QHP) on the Federally-facilitated Exchanges (FFEs) to improve the electronic exchange of health care data, and streamline processes related to prior authorization. The rule requires these payers to take steps to increase patient electronic access to their health care information, and improves the electronic exchange of health information among payers, providers and patients. Together, these policies play a key role in reducing overall payer and provider burden and improving patient access to health information.

This rule includes five key provisions.

Patient Access Application Programming Interface (API)

In the Interoperability and Patient Access final rule (CMS-9115-F), we finalized our policy to require CMS-regulated payers to implement a Fast Healthcare Interoperability Resources (FHIR)-based Patient Access API. In this final rule, starting January 1, 2023, we will require certain regulated payers affected by this rule (and listed above) to include, as part of the previously finalized Patient Access API, claims and encounters, as well as information about the patient's pending and active prior authorization decisions, to ensure patients have a better access to information about the prior authorization process and its impact on their care.

This final rule also requires certain payers to establish, implement, and maintain an attestation process for third-party application developers to attest to certain privacy policy provisions prior to retrieving data via the payer's Patient Access API.

And, this rule requires certain payers to report annual metrics to CMS about patient use of the Patient Access API, which would demonstrate the uptake of the API.

Provider Access APIs

In order to better facilitate coordination of care, and in support of a move to value-based care, we are requiring these impacted payers to build and maintain a Provider Access API for payer-to-provider data sharing of claims and encounter data (not including cost data), a sub-set of clinical data as defined in the U.S. Core Data for Interoperability (USCDI) version 1, and pending and active prior authorization decisions for both individual patient requests and groups of patients

starting January 1, 2023 (for Medicaid managed care plans and CHIP managed care entities, by the rating period beginning on or after January 1, 2023).

Documentation and Prior Authorization Burden Reduction through APIs

Prior authorization is an administrative process used in healthcare whereby a provider must obtain approval from a payer before providing care and prior to receiving payment for delivering items or services. While prior authorization has its benefits, patients, providers, and payers alike have experienced burden from it. And, it has been identified as a major source of provider burden. Providers expend staff resources to identify prior authorization requirements and navigate the submission and approval processes, resources that could otherwise be directed to clinical care. Patients may unnecessarily pay out-of-pocket or abandon treatment altogether when prior authorization is delayed. In an attempt to alleviate some of the administrative burden of prior authorization and to improve the patient experience, we are finalizing a number of policies to help make the prior authorization process more efficient and transparent.

Document Requirements Lookup Service (DRLS) API: We are requiring these impacted payers to build and maintain a FHIR-based DRLS API -- that could be integrated with a provider's electronic health record (EHR) -- to enable providers to electronically locate prior authorization requirements for each specific payer from within the provider's workflow.

Prior Authorization Support (PAS) API: We are requiring these impacted payers to build and maintain a FHIR-based electronic Prior Authorization Support API that would facilitate sending prior authorization requests and receiving responses electronically within their existing workflow (while maintaining the integrity of the HIPAA transaction standards).

Denial Reason: We are requiring these impacted payers to include a specific reason for a denial when denying a prior authorization request, regardless of the method used to send the prior authorization decision under existing law, to facilitate better communication and understanding between the provider and payer.

Shorter Prior Authorization Timeframes: We are requiring these impacted payers (not including issuers of individual market medical QHPs on the FFEs) to send prior authorization decisions, both through the PAS API and as otherwise required by existing requirements, within 72 hours for urgent requests and 7 calendar days for standard requests.

Prior Authorization Metrics: We are requiring these impacted payers to provide transparency by publicly reporting on the operational outcomes of the use of the plan's prior authorization policies and practices.

These prior authorization policies take effect January 1, 2024, with the initial set of metrics to be reported by March 31, 2024 (for Medicaid managed care plans and CHIP managed care entities, by the rating period beginning on or after January 1, 2024).

Payer-to-Payer Data Exchange on FHIR

In the Interoperability and Patient Access final rule (CMS-9115-F), we finalized a requirement that, at a patient's request, CMS-regulated payers must exchange certain patient health information, and maintain that information, thus creating a longitudinal health record for the patient that is maintained with their current payer. While we encouraged the use of a FHIR-based API for this data exchange, we did not require it. In this final rule, we are expanding on this concept to increase data flow among the group of payers to which this rule applies, and to improve patient access to their health information with the following additional requirements:

Payer-to-Payer API: This final rule requires the payers it regulates to exchange patient data via a FHIR-based Payer-to-Payer API, and in addition to a sub-set of clinical data as defined in the USCDI version 1, these payers are now required to exchange claims and encounter data (not including cost data), and information about pending and active prior authorization decisions, at a patient's request.

Payer-to-Payer Data Exchange at Enrollment: We are requiring that the payers the final rule regulates share claims and encounter data (not including cost data), a sub-set of clinical data as defined in the USCDI version 1, and information about pending and active prior authorization decisions at enrollment, for payers that have a specific annual open enrollment period, or during the first calendar quarter of each year, allowing patients to take their health information with them as they move from one payer to another.

These policies take effect January 1, 2023 (for Medicaid managed care plans and CHIP managed care entities, by the rating period beginning on or after January 1, 2023).

Adoption of Health IT Implementation Specifications

On behalf of HHS, the Office of the National Coordinator for Health IT (ONC) adopted the implementation specifications described in this regulation at 45 CFR 170.215—Application Programming Interfaces—Standards and Implementation Specifications as implementation specifications for health care operations. ONC is adopting these implementation specifications on behalf of HHS as part of a nationwide health information technology infrastructure that supports reducing burden and health care costs and improving patient care. By ONC adopting these implementation specifications in this way, CMS and ONC together work to ensure a unified approach to advancing standards in HHS that adopts all interoperability standards in a consistent manner, in one location, for use by individuals and entities in the public and private sectors. Adopting the specified implementation guides (IGs) to support implementation of the APIs is expected to ensure full interoperability of the APIs and reduce implementation burden.

The final rule is available to review today at: https://www.cms.gov/files/document/11521-provider-burden-promoting-patients-electronic-access-health-information-e-prior.pdf

FOR IMMEDIATE RELEASE
January 19, 2021

Contact: HHS Press Office
202-690-6343
media@hhs.gov

HHS Announces New Synthetic Health Data Challenge

The U.S. Department of Health and Human Services' (HHS) Office of the National Coordinator for Health Information Technology (ONC) today announced the launch of the Synthetic Health Data Challenge (Challenge).

Synthetic health data is realistic (but not real) health record data that contains a complete medical history from birth to death. This data can be used without cost or restriction and is intended to support the specific interests of researchers and developers for testing the effectiveness of tools, algorithms, and disease modeling approaches. The Challenge, part of ONC's Synthetic Health Data Generation to Accelerate Patient-Centered Outcomes Research (PCOR) project, invites participants to create and test innovative and novel solutions that will further cultivate the capabilities of Synthea™, an open-source synthetic patient generator that models the medical histories of synthetic patients.

The Synthetic Health Data Challenge encourages researchers and developers to validate the realism of synthetic health records generated by Synthea, develop or improve the disease-progression and treatment modules used to create synthetic records, and spur novel uses of synthetic health data.

"Synthetic data like those created by Synthea can augment the infrastructure for patient-centered outcomes research by providing a source of low risk, readily available, synthetic data that can complement the use of real clinical data," said Teresa Zayas-Cabán, ONC chief scientist. "By enhancing Synthea with new clinical data modules or demonstrating novel uses of Synthea-generated synthetic data, Challenge participants will support PCOR research and development efforts by enhancing PCOR researchers' ability to conduct rigorous analyses and generate relevant findings."

Participants can submit their Challenge Phase I proposals in one of two categories: Enhancements to Synthea or Novel Uses of Synthea Generated Synthetic Data. The best proposals will move on to Challenge Phase II—Prototype or Solutions Development. Phase II features awards totaling up to $100,000: up to two first-place winning solutions will receive $25,000 each; up to two second-place solutions will receive $15,000 each, and up to two third-place solutions will receive $10,000 each.

The Challenge is one in a portfolio of projects ONC is leading to enable PCOR through technology; projects are funded through the Patient-Centered Outcomes Research Trust Fund and managed by the Office of the Assistant Secretary for Planning and Evaluation.

To follow or register for the Synthetic Health Data Challenge or to register for the Phase I Informational Webinar, go to www.challenge.gov/challenge/synthetic-health-data-challenge

For more information about the Synthetic Health Data Generation to Accelerate PCOR project, go to https://www.healthit.gov/topic/research-evaluation/synthetic-health-data-generation-accelerate-patient-centered-outcomes

For more information about ONC's portfolio of PCOR projects go to https://healthit.gov/pcor

###

Broad Coalition of Health and Technology Industry Leaders Announce Vaccination Credential Initiative to Accelerate Digital Access to COVID-19 Vaccination Records

- The Vaccination Credential Initiative (VCI) is working to enable individuals vaccinated for COVID-19 to access their vaccination records in a secure, verifiable and privacy-preserving way.
- Coalition partners include CARIN Alliance, Cerner, Change Healthcare, The Commons Project Foundation, Epic, Evernorth, Mayo Clinic, Microsoft, MITRE, Oracle, Safe Health, and Salesforce.
- The coalition is developing a standard model for organizations administering COVID-19 vaccines to make credentials available in an accessible, interoperable, digital format.
- Trustworthy, traceable, verifiable, and universally recognized digital record of vaccination status is urgently needed worldwide to safely enable people to return to work, school, events, and travel.

January 14, 2021 07:00 AM Eastern Standard Time

NEW YORK--(BUSINESS WIRE)--A broad coalition of health and technology leaders today announced the creation of the Vaccination Credential Initiative (VCI), committed to empowering individuals with digital access to their vaccination records based on open, interoperable standards.

“SAFE is currently working with Hedera to develop a blockchain-enabled crowd safety solution using the VCI standards designed to help get concerts and sporting events going again.”

The current vaccination record system does not readily support convenient access, control and sharing of verifiable vaccination records.

VCI coalition members are working to enable digital access to vaccination records using the open, interoperable SMART Health Cards specification, based on W3C Verifiable Credential and HL7 FHIR standards.

VCI’s vision is to empower individuals to obtain an encrypted digital copy of their immunization credentials to store in a digital wallet of their choice. Those without smartphones could receive paper printed with QR codes containing W3C verifiable credentials.

“The goal of the Vaccination Credential Initiative is to empower individuals with digital access to their vaccination records so they can use tools like CommonPass to safely return to travel, work, school, and life, while protecting their data privacy,” said Paul Meyer, CEO of The Commons Project Foundation. “Open standards and interoperability are at the heart of VCI's

efforts and we look forward to supporting the World Health Organization and other global stakeholders in implementing and scaling open global standards for health data interoperability."

"As we explore the many use cases for the vaccination credential, we are working to ensure that underserved populations have access to this verification," said Dr. Brian Anderson, chief digital health physician at MITRE. "Just as COVID-19 does not discriminate based on socio-economic status, we must ensure that convenient access to records crosses the digital divide. MITRE is an independent advisor and trusted source for managing third-party data and proud to be joining with The Commons Project and other coalition members to deliver an open-source credential."

"A secure, convenient solution to verify COVID-19 vaccination will play an important role in accelerating a healthy and safe return to work, school and life in general," said Joan Harvey, president of care solutions at Evernorth, Cigna's health services business. "Evernorth is helping to lead this important work because the digital vaccine certification made possible by this collaboration will put people in charge of their own health data through innovative technology. It furthers our mission to tackle healthcare's biggest challenges."

"As the world begins to recover from the pandemic, having electronic access to vaccination, testing, and other medical records will be vital to resuming travel and more," said Mike Sicilia, executive vice president of Oracle's Global Business Units. "This process needs to be as easy as online banking. We are committed to working collectively with the technology and medical communities, as well as global governments, to ensure people will have secure access to this information where and when they need it."

"Salesforce is proud to join the Vaccination Credential Initiative to help organizations easily and safely customize all aspects of the vaccination management lifecycle and integrate closely with other coalition members' offerings, which will help us all get back to public life," said Bill Patterson, executive vice president and general manager, CRM Applications at Salesforce. "With a single platform to help deliver safe and continuous operations and deepen trust with customers and employees, this coalition will be crucial to support public health and wellbeing."

"The standards being developed by the Vaccination Credential Initiative, combined with availability of inexpensive smartphone-enabled rapid tests the FDA is now beginning to authorize for home use, will enable application developers to create privacy-preserving health status verification solutions that can be seamlessly integrated into existing ticketing workflows," said Ken Mayer, founder and CEO of Safe Health. "SAFE is currently working with Hedera to develop a blockchain-enabled crowd safety solution using the VCI standards designed to help get concerts and sporting events going again."

"Cerner is already providing tools to clinics, hospitals and other venues that provide health care to support the rapid COVID-19 vaccination process and ensure a safe, streamlined experience. This initiative will grow the standards around data exchange and help patients have access to and easily share verified vaccination information via their mobile device in situations where proof-of-vaccine is necessary," said David Bradshaw, senior vice president of Consumer and Employer Solutions, Cerner. "Cerner is committed to continuing to be an industry advocate for standards-based access to health information."

"We are kicking off the most significant vaccination effort in the history of the United States. Now more than ever, individuals need access to their own vaccination and health information in a portable format to begin to move about the country safely and comfortably," said Ryan Howells, principal, Leavitt Partners and program manager of the CARIN Alliance. "The CARIN Alliance is supportive of MITRE's effort to provide individuals with access to their vaccination information in a secure and trusted way and looks forward to advising the VCI initiative on ways to leverage the CARIN code of conduct and other best practices to facilitate consumer-directed exchange that we have developed consensus on over the last few years."

The Vaccination Credential Initiative has created an informational website at vaccinationcredential.org for more information.

Note to editors

- The Commons Project Foundation queries should be addressed to Samantha Pierce, samantha@120over80mktg.com
- MITRE media inquiries should be addressed to media@mitre.org
- Evernorth media inquiries should be addressed to media@evernorth.com

Contacts

The Commons Project Foundation
Samantha Pierce
samantha@120over80mktg.com

MITRE Media:
media@mitre.org

Evernorth Media
media@evernorth.com

THE
NATIONAL LAW REVIEW

Attachment #5

Cheers to Heightened Health (Privacy) in 2021

GT GreenbergTraurig
Article By
Kate Black
Greenberg Traurig, LLP
Alerts

- Health Law & Managed Care
- Communications, Media & Internet

- All Federal

Tuesday, January 19, 2021

Much changed in the privacy law landscape in 2020, including a heightened focus on the use and disclosure of health information. As 2021 gets underway, businesses should be aware of the key legislative and regulatory changes in health data privacy that were teed up at the close of 2020, and which may now or soon affect them.

HIPAA Proposed Rulemaking

The Office for Civil Rights at the U.S. Department of Health and Human Services (HHS) released proposed changes to the HIPAA Privacy Rule on Dec. 10, 2020. The proposed changes focus on strengthening individuals' access to their health information, facilitating greater caregiver involvement in the care for individuals, and improving access to protected health information (PHI) during emergencies or health crises. There are five primary things to consider in the proposal:

1. HIPAA-covered entities' current 30-day required response time to give individuals access to their PHI would be cut to 15 days.

2. The modifications would create a mechanism for individuals to direct sharing of their PHI among covered health care providers and health plans.

3. The proposed changes aim to strengthen patient access to their PHI by permitting individuals to inspect their PHI in-person, including taking notes or using other personal devices to view and capture images of their records.

4. The proposed rule would require specifications for when electronic PHI must be provided to the individual at no charge.

5. The changes would require HIPAA-covered entities to post estimated fee schedules on their websites for both PHI access and disclosures with an individual's valid authorization as well as provide individualized estimates of fees for an individual's request for copies of PHI.

Public comments will be due 60 days after publication of the proposal in the Federal Register.

California's Consumer Privacy Act (CCPA)

While the CCPA excludes PHI processed under HIPAA (and medical information protected by the California Confidentiality of Medical Information Act), health care and life sciences companies may nevertheless find themselves subject to the law due to data processing activities outside of their health privacy compliance programs, such as:

- Non-PHI health data, including:

– health and wellness information collected from an individual (wearable devices and mobile apps);

– employment records (especially in light of myriad COVID-19 employer-testing programs);

- De-identified PHI, i.e., data de-identified under HIPAA that may still be personal information under the CCPA due to it being capable of re-identification; and
- Inferences drawn from PHI that can be reasonably linked to an individual.

On Sept. 25, 2020, the California governor signed into law AB 713, which amends the CCPA's HIPAA exception in a number of ways. AB 713 makes an exception for "business associates" under HIPAA; clarifies that the CCPA does not apply to data that was de-identified pursuant to HIPAA standards and derived from patient information originally collected by a HIPAA-regulated entity; expands the scope of the CCPA's health research exceptions to cover studies other than clinical trials; prohibits re-identification of de-identified patient information; and imposes new contracting and notice requirements for certain disclosures of de-identified patient information. AB 713 became operative immediately, except for the law's new contractual requirements that went into effect Jan. 1, 2021.

The health-related exceptions under the CCPA will still be carved out under the recently passed California Privacy Rights Act (CPRA). As such, health companies can get ahead of CPRA compliance by taking actions to comply with the CCPA and AB 713 now.

Health Information Blocking Rules Extended

In November 2020, the HHS Office of the National Coordinator for Health Information Technology (ONC) published an Interim Final Rule: Information Blocking and the ONC Health IT Certification Program: Extension of Compliance Dates and Timeframes in Response to the COVID-19 Public Health Emergency (Interim Final Rule) providing relief to entities working toward compliance with the 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program Final Rule (ONC Rule), issued May 1, 2020. The Interim Final Rule provides regulated entities with "additional flexibilities" to implement the provisions of the ONC Rule including updated compliance dates. ONC explained that the extension is due to the COVID-19 public health emergency.

On Jan. 4, ONC released new resources and guidelines for requirements related to its upcoming information-blocking rules.

COVID-19 Vaccine Reporting

The Centers for Disease Control and Prevention is instructing states to sign data use agreements that commit them for the first time to sharing personal information related to COVID-19 vaccinations in existing state registries with the federal government. States normally collect this type of data themselves, but some are pushing back against giving it to federal authorities due to privacy and data use concerns, with Minnesota and Colorado, for example, saying they will only share de-identified data. Other states, such as New York, are refusing to sign or share the information at all.

Sen. Klobuchar Seeks Consumer Health Privacy Protections

Sen. Amy Klobuchar (D-Minn.) has asked HHS to provide more consumer privacy protection in response to new wearable health devices. On Dec. 11, 2020, Sen. Klobuchar sent a letter to HHS Secretary Alex Azar asking what HHS is doing to ensure such devices safeguard sensitive health information. In 2019, Klobuchar sponsored legislation with Sen. Lisa Murkowski (R-Alaska) to regulate tracking devices, health apps and home DNA testing kits. The Protecting Personal Health Data Act proposed that the HHS secretary create regulations for new direct-to-consumer health regulations not covered by existing laws.

FBI and HHS Release Ransomware Alert

On Nov. 2, 2020, the Cybersecurity and Infrastructure Security Agency (CISA), FBI, and HHS jointly released the Ransomware Activity Targeting the Healthcare and Public Health Sector Alert (the Alert). The Alert provides extensive detail regarding the mechanism and indicators of Trickbot malware. Trickbot is used to deploy Ryuk ransomware, which has reportedly recently forced multiple hospitals across the country offline in a coordinated attack. The Alert includes best practices for health care providers to minimize risk and mitigate harm, including the following critically important practices:

1. Implement business continuity plans – or plans to continue essential functions through emergencies such as cyberattacks and to minimize service disruptions;
2. Maintain formal and informal training and security awareness programs, covering ransomware and phishing scams;
3. Patch system, software, and firmware as new patches are released;
4. Require regular password changing; and
5. Implement multi-factor authentication.

The Alert also includes some ransomware best practices, such as:

- Do not pay the ransom (payment does not guarantee that files will be recovered, and it emboldens cyber criminals);
- Regularly back up data and secure backup copies offline;
- Engage with CISA, FBI, and HHS for information-sharing, best practices, and other resources;
- Retain three copies of all critical data on at least two different types of media with at least one stored offline.

National Law Review, Volume XI, Number 19

FTC Reaches Settlement With Flo Health Over Fertility-Tracking App

John D. McKinnon
The Wall Street Journal
1/14/21

WASHINGTON—The Federal Trade Commission reached a settlement with Flo Health Inc., the developer of a widely used period and fertility-tracking app, over allegations that it improperly shared personal data with Facebook and others, including whether users were ovulating.

The data shared by Flo Health often allowed online ads to be targeted to those users, despite Flo Health's promises that the information would be kept private, The Wall Street Journal found in a 2019 article.

The FTC's vote on the proposed settlement was 5-0, the agency said Wednesday. The proposed settlement with the FTC, if it becomes final following public comment, would require Flo Health to obtain an independent review of its privacy practices and get users' consent before sharing their health information, the agency said. The company also must notify consumers of the FTC charges that it shared consumers' personal information without their consent, commissioners said.

In a statement, a Flo spokesperson said the company cooperated with the FTC, adding, "We are committed to ensuring that the privacy of our users' personal health data is absolutely paramount."

The company emphasized that it didn't share users' names, addresses or birthdays, and that its agreement with the FTC wasn't an admission of wrongdoing but allowed it to "avoid the time and expense of litigation and...decisively put this matter behind us."

The FTC alleged in its complaint that Flo promised to keep users' data private, when it actually disclosed data to third parties that provided marketing and analytics services to the app, including Facebook's analytics division as well as Alphabet Inc.'s Google analytics division and others.

Facebook didn't respond to a request for comment. Google didn't respond prior to publication, but after this article was published, a Google spokesperson said companies that use Google Analytics on their websites and apps own all data collected by the service and can delete that data at any time.

"We don't build advertising profiles from sensitive data like health conditions, and we have strict policies preventing developers and advertisers from using such data to personalize ads," the spokesperson said.

Flo didn't stop disclosing this data until its practices were revealed in the 2019 Wall Street Journal article, according to the agency. The Journal's testing showed that Facebook software collected data from many apps even if no Facebook account was used to log in, and even if the end user wasn't a Facebook member.

The article prompted "hundreds" of complaints from users, the FTC said.

The FTC suggested that more such cases could be coming.

"Apps that collect, use and share sensitive health information can provide valuable services, but consumers need to be able to trust these apps," said Andrew Smith, director of the FTC's Bureau of Consumer Protection. "We are looking closely at whether developers of health apps are keeping their promises and handling sensitive health information responsibly."