Consumer Health Privacy: Navigating The Digital Health Frontier

Libbie Canter & Jacob Smith

November 2023

COVINGTON

BEIJING BOSTON BRUSSELS DUBAI FRANKFURT JOHANNESBURG LONDON
LOS ANGELES NEW YORK PALO ALTO SAN FRANCISCO SEOUL SHANGHAI WASHINGTON

www.cov.com

The Promise of Digital Health

Johns Hopkins Bloomberg School of Public Health

Consumer Electronics Can Help Improve Patient Health

NEWS • HEALTH NEWS

How Fitness Trackers Can Help Reduce Afib and Stroke Risk

National Library of Medicine
National Center for Biotechnology Information

Consumer health informatics approach for personalized cancer screening decisions using utility functions

Federal Communications Commission

Connected Health Technology Can Help in the Fight Against Cancer

Imperial College London

Wearable tech, AI and clinical teams join to change the face of trial monitoring

New mHealth Intervention Aims to Curb Smoking Among Black HIV Patients

University of Houston researchers have launched a research project to study whether an mHealth app intervention can help Black patients with HIV quit smoking.

Agenda

1. Overview & Key Trends
2. Practice Pointers: How To Navigate the Digital Health Frontier
    - What Is Health Information?
    - When Should You Seek Consent or Authorization?
    - What Should Consent or Authorization Look Like?
    - Data Breach Notification
    - Other Practice Pointers

Overview & Key Trends

Exemplar U.S. Privacy Frameworks

General Privacy Frameworks

- FTC Act
- CCPA and similar state laws
- CAN-SPAM, TCPA and marketing rules
- Biometric privacy, location privacy, etc.

Health Privacy Laws in Clinical Context

- HIPAA
- CMIA and similar state laws
- Genetic Testing/ Privacy Laws

Health Privacy Outside Clinical Context

- Washington My Health My Data and similar laws
- FTC Breach Notification Rule
- Genetic Testing/ Privacy Laws

Underlying Privacy Trends

Federal and state policymakers and regulators are concerned about and focused on health data that is not regulated under HIPAA and human subject research laws

There is still no clear definition of consumer health data. Even as we see some alignment in definitions, it often is context- or purpose dependent.

The FTC has brought four cases in recent years alleging that digital health tools violated law through use of ad tech solutions; there has also been a wave of litigation involving ad tech by health systems and other companies.

A number of states have enacted laws regulating the collection and use of genetic data, some in the context of direct-to-consumer genetic testing companies

***Dobbs* continues to influence the landscape, with greater attention by policymakers and regulators to women's health and geolocation data**

Practice Pointers: How To Navigate the Digital Health Frontier

What is Health Information?

Washington My Health My Data Act

"**Consumer health data** means personal information that is linked or reasonably linkable to a consumer and that identifies the consumer's past, present, or future physical or mental health status."

Includes:

- Individual health conditions, treatment, diseases, or diagnosis
- Gender-affirming care information
- Biometric data
- Precise location information
- Data that identifies a consumer seeking health care services

HIPAA

"**Individually identifiable health information** means any information, including demographic information collected from an individual, that— (A) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and—

(i) identifies the individual; or

(ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual."

FTC Consent Orders

"individually identifiable information relating to the health or genetics of an individual"

In the Matter of Health.io Inc. (2023)

"medical records and other individually identifiable information relating to the past, present, or future physical or mental health or conditions of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual."

U.S. v. Easy Healthcare (2023)

"individually identifiable information from or about an individual consumer relating to health, including but not limited to information concerning fertility, menstruation, sexual activity, pregnancy, and childbirth"

In the Matter of Flo Health, Inc. (2021)

Virginia Consumer Data Protection Act

"**Personal data** means any information that is linked or reasonably linkable to an identified or identifiable natural person."

"**Sensitive data** means a category of personal data that includes:

- Mental or physical health diagnosis
- Genetic or biometric data for the purpose of uniquely identifying a natural person"

Are there certain types of information that are higher risk?

When Should You Seek Consent or Authorization?

Standard	WA My Health My Data	Health Breach Notification Rule	Other Litigation
	Collection – prior consent for specified purpose unless reasonably necessary to provide requested service **Sharing** – prior consent, separate from consent to collection, unless reasonably necessary to provide requested service **Selling** – prior authorization required, separate from consents	**Breach of security** – "acquisition of such information without the authorization of the individual." • FTC considers *any* unauthorized disclosure to constitute a breach of security, not just those that result from bad actors, cybersecurity incidents.	**Ex. Pixel cases** – allegations that pixel collected information from health care provider and hospital websites, including those that require a log in **Potential causes of action:** State/federal wiretap laws HIPAA Negligence Invasion of privacy Breach of Contract Breach of Fiduciary Duty

What Should Consent or Authorization Look Like?

WA: MHMDA

Consent – "A clear affirmative act that signifies a consumer's freely given, specific, informed, opt-in, voluntary, and unambiguous agreement"

Authorization – "a document written in plain language" signed by the consumer that includes specific health data, seller and purchaser information, description of purpose of sale, statement of consumer's rights, expiration date.

CA: CMIA

- Specific uses and limitations on the use of the medical information
- Expiration date of authorization
- Signature with no other purpose other than authorization
- Handwritten by signer or typed in at least 14-point font

Data Breach Notification

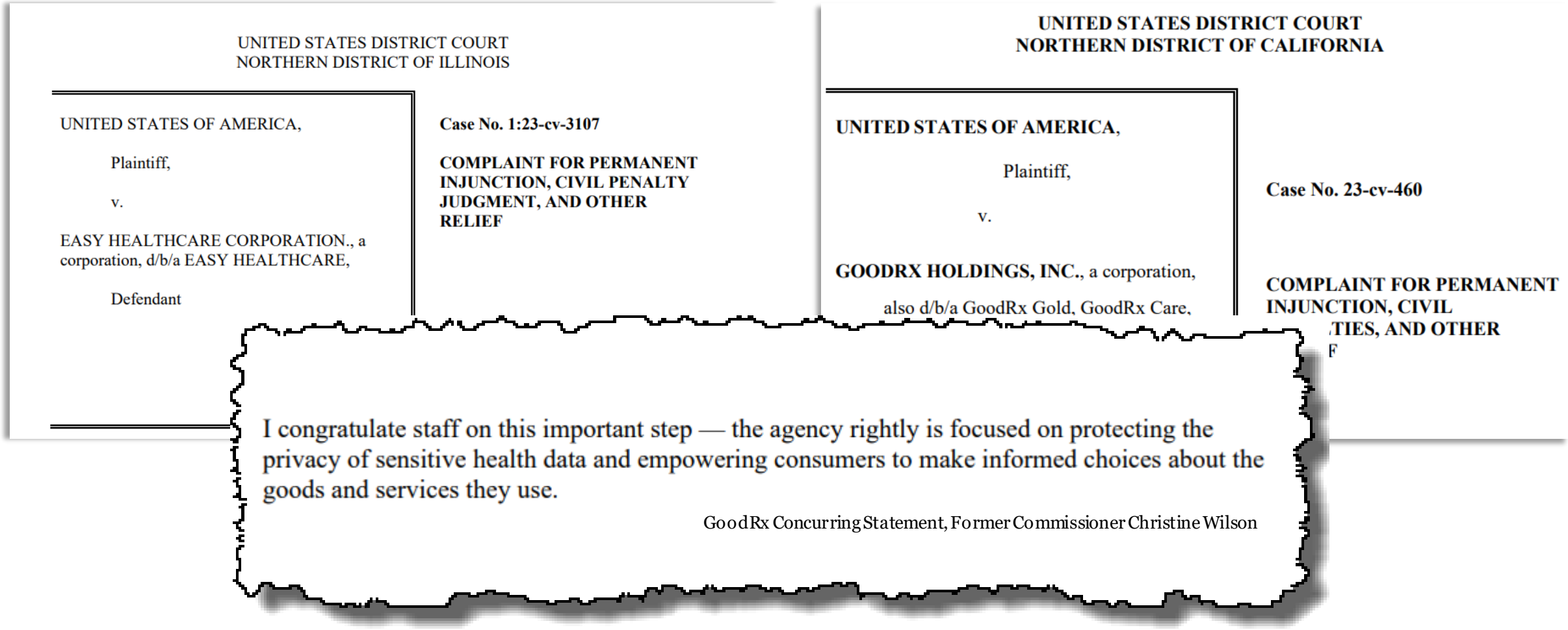
FTC HBNR: "[E]ach **vendor of personal health records**, following the discovery of a **breach of security of unsecured PHR identifiable health information** that is in a personal health record maintained or offered by such vendor, and each PHR related entity, following the discovery of a **breach of security** of such information that is obtained through a product or service provided by such entity, shall:

(1) **Notify each individual** who is a citizen or resident of the United States whose unsecured PHR identifiable health information was acquired by an unauthorized person as a result of such breach of security; and

(2) **Notify the Federal Trade Commission**."

16 C.F.R. § 318.3

Data Breach Notification



UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS

UNITED STATES OF AMERICA,

Plaintiff,

v.

EASY HEALTHCARE CORPORATION., a corporation, d/b/a EASY HEALTHCARE,

Defendant

Case No. 1:23-cv-3107

COMPLAINT FOR PERMANENT INJUNCTION, CIVIL PENALTY JUDGMENT, AND OTHER RELIEF

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA,

Plaintiff,

v.

GOODRX HOLDINGS, INC., a corporation,

also d/b/a GoodRx Gold, GoodRx Care,

Case No. 23-cv-460

COMPLAINT FOR PERMANENT INJUNCTION, CIVIL
TIES, AND OTHER
F

I congratulate staff on this important step — the agency rightly is focused on protecting the privacy of sensitive health data and empowering consumers to make informed choices about the goods and services they use.

GoodRx Concurring Statement, Former Commissioner Christine Wilson

Other Practice Pointers?

- Training and awareness
- Building relationships
- Understanding the technology
  - Ad tech
- Leveraging international processes
- Tracking key developments

APPENDIX

Washington My Health My Data Act, Nevada, SB 370, and Connecticut amendments

Washington – My Health My Data Act (HB 1155)

Scope: Governs "consumer health data"

Exemptions: PHI under HIPAA, Part 2 information, certain research information, HIPAA de-identified information, among others

Enforcement: AG and private right of action

Transparency: Must publish a privacy policy for consumer health data

Consumer Rights: (1) access*; (2) withdraw consent from the collection and sharing of their health data; and (3) deletion

Other Safeguards: Appropriate data security measures, data processing agreements with processors

Consent: Requires consent to collect and separate consent to share consumer health data

Authorization: Requires HIPAA-like authorization to sell consumer health data

Prohibitions: Prohibits geofencing around health care facilities for certain purposes, e.g., to track consumers seeking health care

Connecticut and Nevada

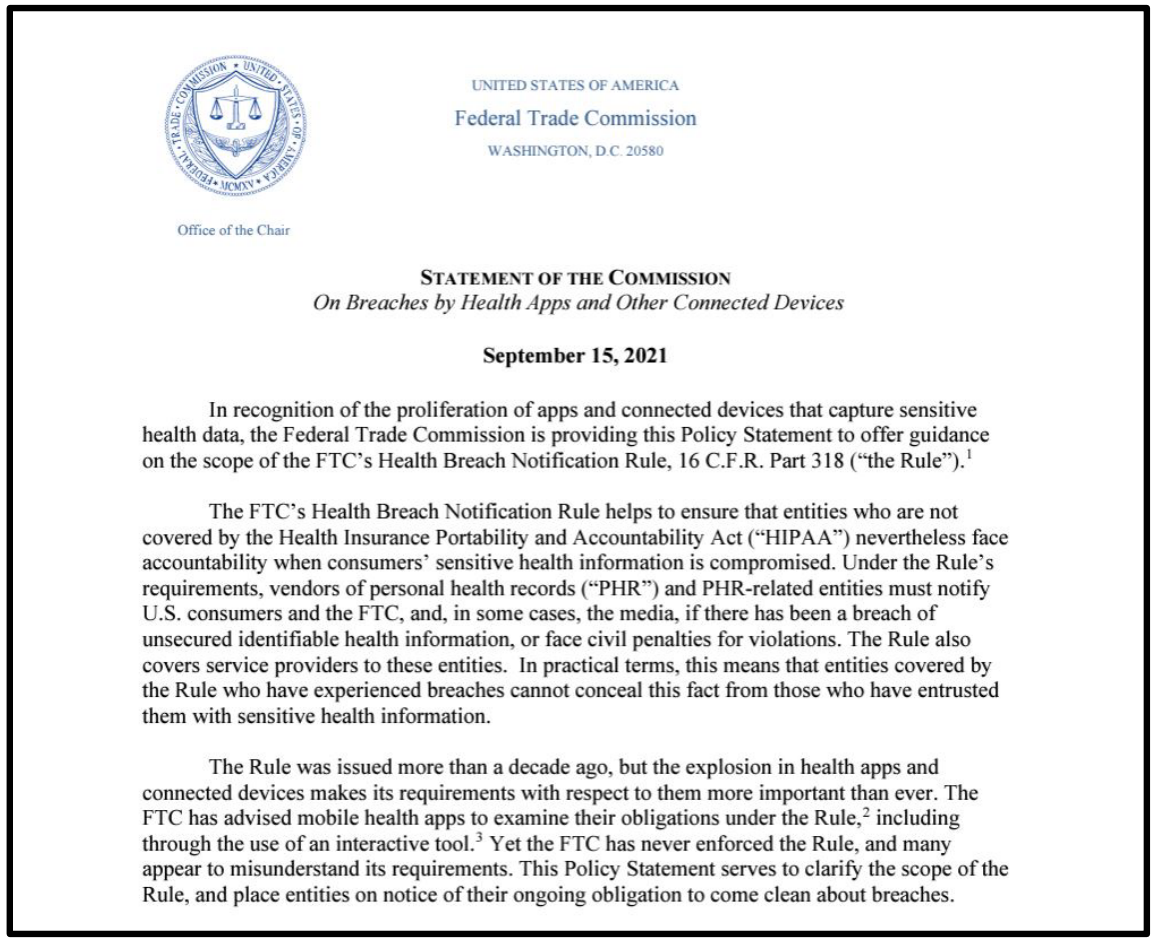
Connecticut
(SB 3)

Nevada
(SB 370)

- Nevada is similar to Washington, although (1) it gives consumers a slightly broader right to request entity cease collecting, sharing, or selling consumer health data, (2) it does not have a private right of action, and (3) it is missing some express exemptions.
- Connecticut amended its general consumer privacy law, so the scope of consumer rights under similar

FTC Breach Notification Rule & Recent FTC Enforcement

September 2021 Policy Statement



UNITED STATES OF AMERICA
Federal Trade Commission
WASHINGTON, D.C. 20580

Office of the Chair

STATEMENT OF THE COMMISSION
On Breaches by Health Apps and Other Connected Devices

September 15, 2021

In recognition of the proliferation of apps and connected devices that capture sensitive health data, the Federal Trade Commission is providing this Policy Statement to offer guidance on the scope of the FTC's Health Breach Notification Rule, 16 C.F.R. Part 318 ("the Rule").[1]

The FTC's Health Breach Notification Rule helps to ensure that entities who are not covered by the Health Insurance Portability and Accountability Act ("HIPAA") nevertheless face accountability when consumers' sensitive health information is compromised. Under the Rule's requirements, vendors of personal health records ("PHR") and PHR-related entities must notify U.S. consumers and the FTC, and, in some cases, the media, if there has been a breach of unsecured identifiable health information, or face civil penalties for violations. The Rule also covers service providers to these entities. In practical terms, this means that entities covered by the Rule who have experienced breaches cannot conceal this fact from those who have entrusted them with sensitive health information.

The Rule was issued more than a decade ago, but the explosion in health apps and connected devices makes its requirements with respect to them more important than ever. The FTC has advised mobile health apps to examine their obligations under the Rule,[2] including through the use of an interactive tool.[3] Yet the FTC has never enforced the Rule, and many appear to misunderstand its requirements. This Policy Statement serves to clarify the scope of the Rule, and place entities on notice of their ongoing obligation to come clean about breaches.

- Clarifies that health app developers may be subject to the rule
- Health apps may be considered PHRs if "they are capable of drawing information from multiple sources, such as through a combination of consumer inputs and application programming interfaces" (e.g., fitness trackers)
- "Breach" is interpreted to include any disclosure of sensitive health information without users' authorization

HBNR Enforcement: GoodRx

- GoodRx lets users keep track of their personal health information (e.g., to save, track, and receive alerts about their prescriptions, refills, pricing, and medication purchase history)
- FTC alleged GoodRx is a vendor of PHRs and that it violated the HBNR and FTC Act by sharing users' personal health information with third-party ad tech tools

California Confidentiality of Medical Information Act

CMIA: "Provider of Health Care"

Cal. Civ. Code § 56.06(b)

Includes, in addition to typical health care providers, any **business that "offers software or hardware to consumers,** including a mobile application or other related device that is designed to maintain medical information…in order to make the information available to an individual or a provider of health care…for purposes of allowing the individual to manage his or her information, or for the diagnosis, treatment, or management of a medical condition of the individual"

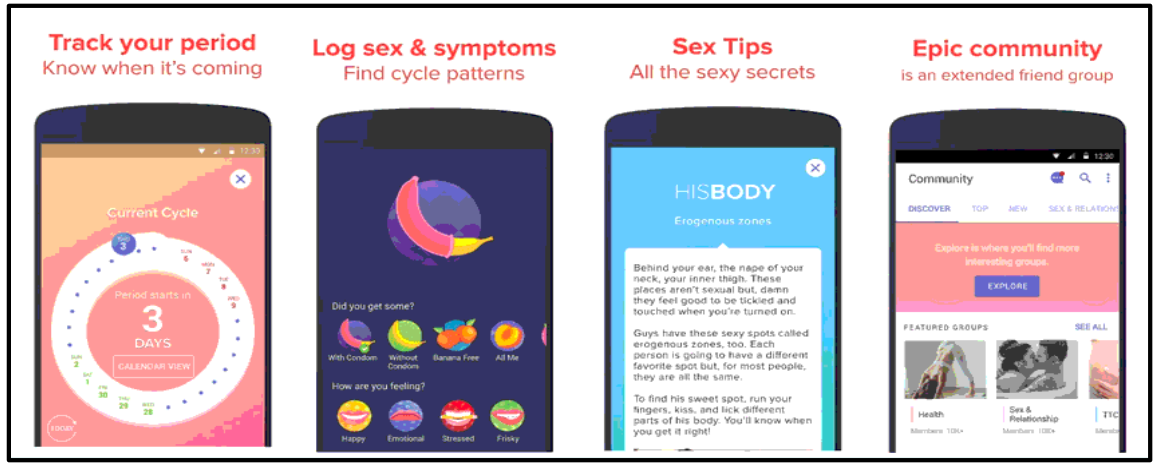
Interpreted to Include

- **CA Attorney General:** Digital health app providers (e.g., fertility tracking apps)
- **SC District Court:** Businesses that maintain medical information, regardless of whether that is the primary purpose of the business and regardless of whether the business offers software or hardware directly to consumers
  - Interpretation part of an out-of-state district court ruling on a MTD

Fertility Tracking Apps: Glow Enforcement (CA)

Glow was found to have violated the CMIA because it:

- Immediately shared sensitive information without verification
- Failed to authenticate old passwords
- Made representations contradicted by privacy practices



Key Takeaways

- Health data is sensitive even if it is not regulated under HIPAA
- App providers may be providers of health care for the purposes of CMIA
- Health information may be "medical information" for the purposes of the CMIA "irrespective of how the information is transmitted," and thus may include information that is "manually enter[ed] or upload[ed] . . . into a mobile application or online service"