HEALTHCARE REGULATORY ROUND-UP #73

The Healthcare Privacy Forecast: Navigating the Regulatory Climate

June 19, 2024

Introductions

Karin Anderson
Principal
kanderson@pyapc.com

Erin Walker
Manager
ewalker@pyapc.com

Reproductive Health Privacy

President's Executive Order to HHS

"[S]trengthen the protection of sensitive information related to reproductive healthcare services and bolster patient-provider confidentiality."

1) July 8, 2022 U.S. President Executive Order 14076 Protecting Access to Reproductive Healthcare Services

Definition of Reproductive Health

- PHI that includes healthcare "that affects the health of an individual in all matters relating to the reproductive system and to its functions and processes."
- Goal is that definition be “interpreted broadly”
  - Examples
    - Contraceptive medications
    - Peri- and post-menopausal treatments
    - Provision of medications and devices, including over-the-counter medications or devices.
- Applicable to reproductive healthcare that is lawful in the state rendered

Final Rule – HIPAA Privacy Rule to Support Reproductive Health Care Privacy, effective June 26, 2024

Strengthens privacy protections for medical records and health information for women, their family members, and doctors who are seeking, obtaining, providing, or facilitating lawful reproductive health care.

Bolsters patient-provider confidentiality and helps promote trust and open communication between individuals and their health care providers or health plans – essential components for high-quality health care.

HHS issued after hearing from communities that changes were needed to better protect patient confidentiality and prevent medical records from being used against people for providing or obtaining lawful reproductive health care.

1) https://www.hhs.gov/sites/default/files/hipaa-privacy-rule-support-reproductive-health-care-privacy.pdf

https://www.hhs.gov/hipaa/for-professionals/special-topics/reproductive-health/final-rule-fact-sheet/index.html

HIPAA Reproductive Health Information Rule Changes

- New “Purpose Based” disclosure prohibition
  - If the purpose of the use or disclosure is for the patient’s healthcare, it is permitted.
  - If the purpose is for a Prohibited Purpose (e.g., to investigate or impose liability on any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care and to identify any person for that purpose), it is not permitted without the patient’s authorization.
- New “Attestation” required for persons seeking reproductive health information who must attest that the information sought is for a HIPAA-compliant purpose
- Notice of Privacy Practices - Incorporate reproductive health related uses and disclosures
- Medical Record Requests - Changes to HIM Process will be required to respond

Final Rule – Use/Disclosure Prohibition is Purpose Based

Prohibits the use or disclosure of protected health information by a covered health care provider, health plan, or health care clearinghouse – or their business associate – for either of the following activities:

- To conduct a criminal, civil, or administrative investigation into or impose criminal, civil or administrative liability on any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care, where such health care is lawful under the circumstances in which it is provided.
- The identification of any person for the purpose of conducting such investigation or imposing such liability

Final Rule – Applicability

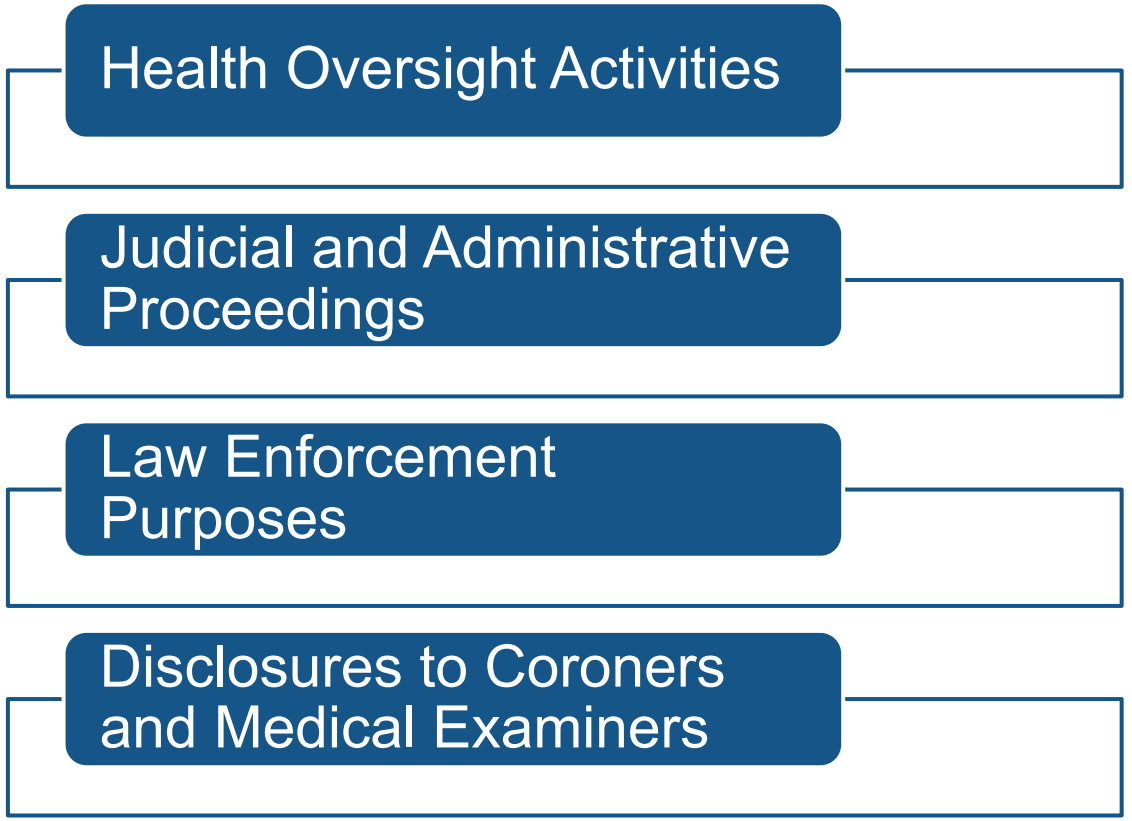
- The reproductive health care is lawful under the law of the state in which such health care is provided under the circumstances in which it is provided
- The reproductive health care is protected, required or authorized by Federal law, including the U.S. Constitution, regardless of the state in which such health care is provided
- The reproductive health care was provided by a person other than the covered health care provider, health plan, or health care clearinghouse (or business associates) that receives the request for PHI and the presumption that the reproductive health care is lawful under the circumstances in which it was provided

Final Rule - Presumption

- The Final Rule includes a presumption that the reproductive health care provided was lawful if provided by a person other than the covered health care provider, health plan or health care clearinghouse (or business associates) receiving the request. (CE did not provide the care, but receives request – presume care is "lawful")
- The reproductive health care is presumed to be lawful **unless the covered entity or business associate**:
  - **Has actual knowledge** that the reproductive health care was not lawful under the circumstances in which it was provided.
  - **Receives factual information** from the person making the request for the use or disclosure of **PHI that demonstrates a substantial factual basis** that the reproductive health care was not lawful under the circumstances in which it was provided.

Final Rule – Attestation

- Upon a medical record request potentially for reproductive health care, the requestor must complete and sign an “Attestation” stating that the use or disclosure is not for a prohibited purpose
- Model Attestation language to be published by December 2024, the deadline for compliance



Final Rule – Notice of Privacy Practices

- Notice of Privacy Practices Revisions
  - Address reproductive health care privacy protections as it relates to disclosure of the information
  - Address proposals made in the Notice of Proposed Rulemaking for the Confidentiality of Substance Use Disorder Patient Records as required by or consistent with the CARES Act of 2020 (HIPAA Part 2).

Final Rule – Disclosures to Law Enforcement

- Covered entities (and business associates), including workforce members, are only permitted to disclose PHI for law enforcement purposes where they suspect an individual of obtaining reproductive health care (lawful or otherwise) if the covered entity or business associate is required to do so and all applicable conditions are met:
  - The disclosure is not subject to the prohibition
  - The disclosure is Required by Law
  - The disclosure meets all applicable conditions of the Privacy Rule permission to use or disclose PHI as Required by Law

HIPAA Privacy Rule – Summary of the changes

Prohibits the use or disclosure of PHI when it is sought to investigate or impose liability on individuals, health care providers, or others who seek, obtain, provide, or facilitate reproductive health care that is lawful under the circumstances in which such health care is provided, or to identify persons for such activities.

Requires a regulated health care provider, health plan, clearinghouse, or their business associates, to obtain a signed attestation that certain requests for PHI potentially related to reproductive health care are not for these prohibited purposes.

Requires regulated health care providers, health plans, and clearinghouses to modify their Notice of Privacy Practices to support reproductive health care privacy.

Enforcement

- Preamble to the Final Rule by OCR
- **Criminal Liability**: a person, including a HIPAA-regulated entity or a person requesting PHI, who **knowingly obtains or discloses** individually identifiable health information in violation of the HIPAA regulations could be subject to criminal liability, which would include a person who falsifies an attestation.
- **Civil Liability**: covered entities and business associates that disclose PHI **without obtaining a valid attestation when one is required** could result in the imposition of civil penalties.

OCR Briefing June 20, 2024: HIPAA Privacy Rule to Support Reproductive Health Care Privacy

- June 20, 2024
- 2 p.m. eastern
- OCR leadership to provide overview of the rule and Q&A
- Registration link: timehttps://capconcorp.zoom.us/webinar/register/WN_QI76yKQnT4Gki15Kf5p0og#/registration

Patient Informed Consent

DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop C2-21-16
Baltimore, Maryland 21244-1850

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES

Center for Clinical Standards and Quality/Quality, Safety & Oversight Group

Ref: QSO-24-10-Hospitals

DATE: **April 1, 2024**

TO: State Survey Agency Directors

FROM: Directors, Quality, Safety & Oversight Group (QSOG) and Survey & Operations Group (SOG)

SUBJECT: Revisions and clarifications to Hospital Interpretive Guidelines for Informed Consent

Conditions of Participation for Informed Consent

For Hospitals - revised survey interpretive guidance to comply with CMS Hospital Conditions of Participation (COP)

New concerns: Whether informed consent was obtained for patients under anesthesia who had sensitive procedures performed by providers/students/residents (medical trainees) for educational purposes.

Sensitive procedures: exams of breast, pelvic, prostate, rectal

CMS took steps: to ensure **hospitals' patient informed consent policy, procedure and informed consent forms** allow for a patient to make fully informed decisions about their care.

Must inform patient if examination/invasive procedure or important task in surgery is performed for "educational and training purposes," which requires consent.

CMS Surveyors Tag A-0955

Medical Record Services 42 CFR 482.24 (c)(4)(v)

Patient Rights

- CMS Hospitals must utilize **informed consent process** that ensures patients are given information needed to make informed decision about whether to consent to a procedure, intervention or type of care that requires consent.
- **Hospital Conditions of Participation:**
  "The patient or his or her representative (as allowed under State law) has the right to make informed decisions regarding his or her care. The patient's rights include being informed of his or her health status, being involved in care planning and treatment, and being able to request or refuse treatment. This right must not be construed as a mechanism to demand the provision of treatment or services deemed medically unnecessary or inappropriate. 42 CFR 482.13(b)(2)

Patient Rights

- Office of Civil Rights (OCR) FAQ
  - Patient requests restriction for use of information as it relates to medical trainees
  - https://www.hhs.gov/hipaa/for-professionals/faq/can-an-individual-restrict-who-has-access-to-their-protected-health-information-during-a-medical-procedure/index.html
- OCR Open Letter to Hospitals
  - Hospitals must set clear guidelines to ensure providers and trainees first obtain and document informed consent from patients before performing sensitive examinations in all circumstances, including when the patient is under anesthesia.

1) Open Letter to Hospitals :https://www.hhs.gov/about/news/2024/04/01/letter-to-the-nations-teaching-hospitals-and-medical-schools.html

To Do List

- Updates - Informed Consent Form
  - Name of person who is performing the procedure/administering treatment
  - Statement that procedure/treatment was explained to patient, specifically, the anticipated benefits, materials risks, alternative therapies
- Hospital policy and procedure for informed consent
- Medical Staff policy on what procedures/treatments require patient consent
- State and federal law consent requirements (e.g., clinical research studies)
- State Operations Manual, Appendix A (interpretive guidance for surveyors),Tags A-0466, A-0131, A-0955 (revised)

State Laws – Consumer Information Privacy

Consumer Information Privacy – State Laws in Play

State Laws in Effect	Effective 2024	Effective 2025	Effective 2026
• California • Colorado • Connecticut • Nevada • Virginia • Utah	• Florida • Montana • Oregon • Texas	• Delaware • Iowa • Maryland • Nebraska • New Jersey • New Hampshire • Tennessee	• Indiana • Kentucky

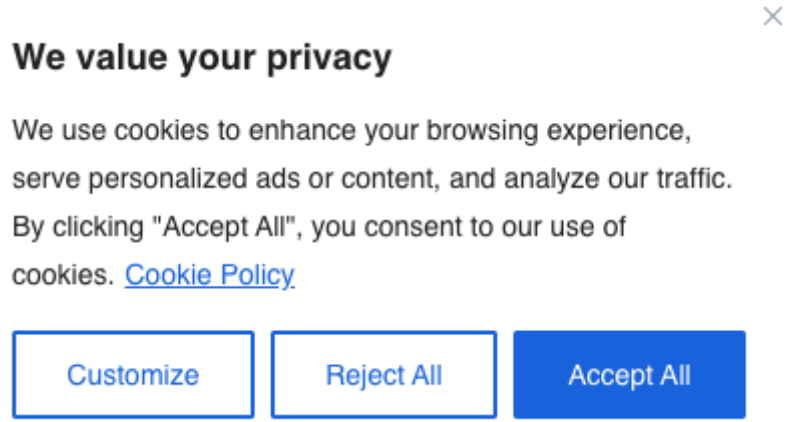
State Consumer Privacy Laws

- Although each state law is different, there is a shared goal to protect a consumer's personal information entered on a website for a transaction from being **sold or disclosed to other organizations** without the **consent of the consumer**
- State law requirements
  - Websites must describe uses and disclosures of consumer's information provided to organization (Privacy Policy)
  - Consumers must consent to the organization's practices before entering the website (Consent)

1) https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html

Consent and Privacy Policy for Consumer Information

Consumer Content



What are Tracking Technologies?

- Script or code on a website or mobile app:
  - Gathers information about users.
    - Many are not apparent to the user
    - Can be developed internally or by third parties
    - Website examples – cookies, web beacons/tracking pixels, session replay scripts, fingerprinting scripts
    - Mobile app examples – tracking codes, mobile device-related information capture (e.g., device/advertising ID)
- Unique identifiers and information collected enable creation of individual profiles about each user.
  - Provides insights about user's online activities.
  - Can be beneficial but can also be subject to misuse.

OCR Bulletin

- Issued December 1, 2022
- Prompted by recent news: regulated entities sharing patient appointment information with social media companies (tracking pixels, etc.)
  - An individual visiting a website is evidence of a relationship or anticipated future relationship between visitor and regulated entity.
- **Generally, all individually identifiable health information (IIHI) collected on a regulated entity's website or by its mobile app is PHI:**
  - Even if the individual does not have an existing relationship with regulated entity
  - Even if the IIHI, such as IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services

Source: https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html#ftn20

Mobile Application Example

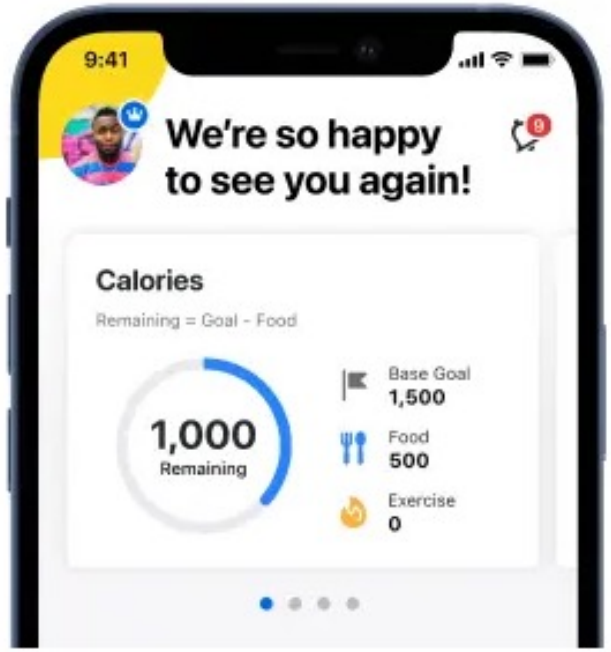
MyFitnessPal iPhone App

Reach your weight loss goals with MyFitnessPal, the best calorie counter on the iPhone. Set a daily calorie goal and record your daily food and exercise to make sure you stay on track. Then watch the pounds come off!

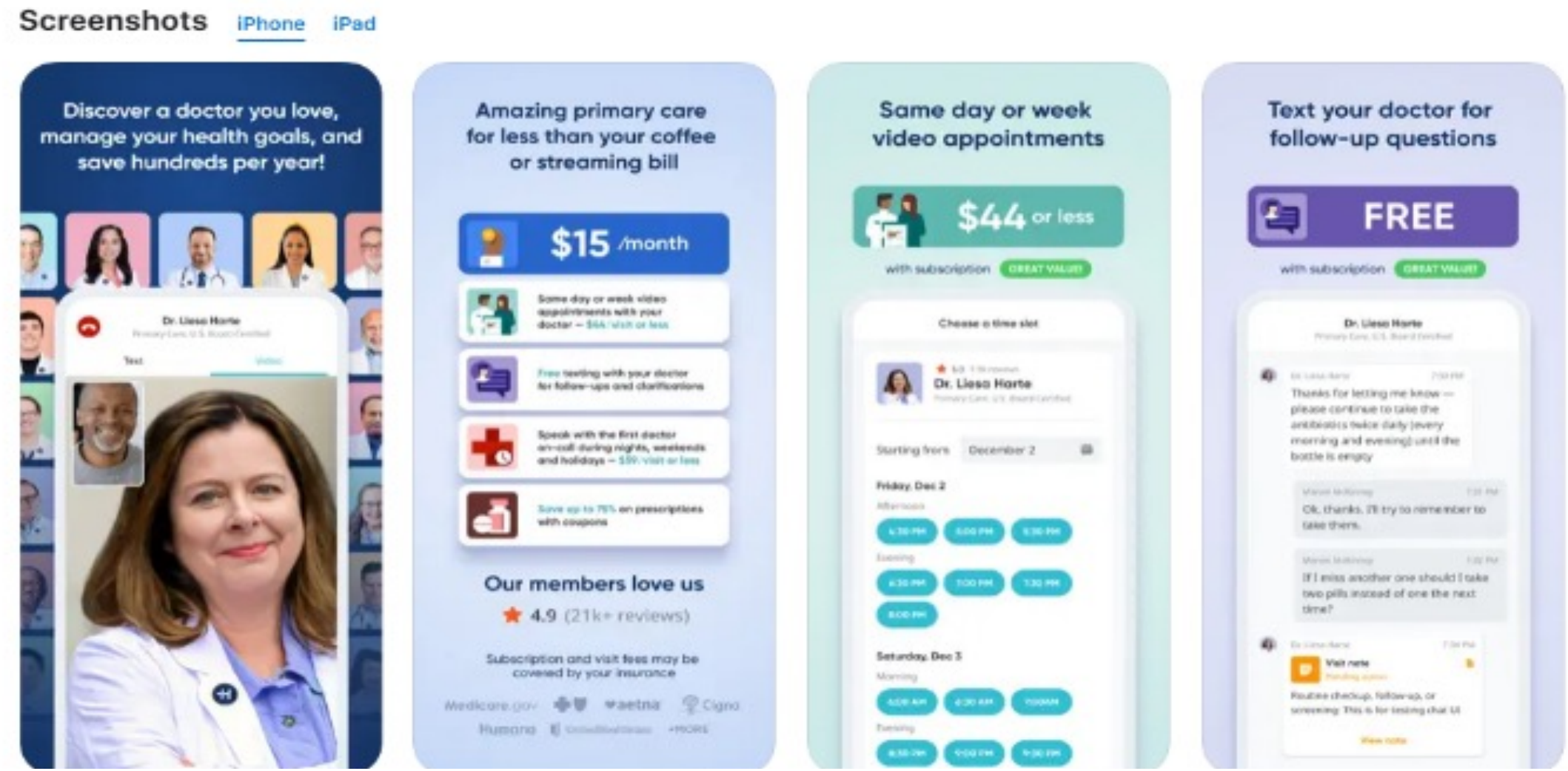
Our iPhone app gives you full mobile access to your MyFitnessPal.com account, so you can log your food and exercise from anywhere, at any time. All changes made on your iPhone will be synchronized with our website and vice versa.

Best of all, both the iPhone app and our website are **FREE!** So don't wait - start changing your life today.

Download on the App Store



Mobile Application Example



Mobile Applications – when HIPAA is not implicated

- **HIPAA Rules do not protect the privacy and security of information that users voluntarily download or enter into a mobile application that is not developed or offered by or on behalf of a regulated entity, regardless of where the information came from.**
  - Example: health information entered into a mobile application offered by an entity not regulated by HIPAA – even if information was obtained from an individual's medical record
- Other laws may apply: FTC

Consumer Information Privacy State Laws and HIPAA

Intersection with HIPAA:

If states provide greater (stricter) privacy protections for individually identifiable health information than HIPAA; ***or***

If states provide additional privacy rights beyond HIPAA

Recommendations:

Review state law to determine if your state has a consumer information privacy law

Incorporate any state law requirements related to privacy of individually identifiable health information into your privacy policies and procedures

Federal Trade Commission
Updated Health Breach Notification Rule

https://www.ftc.gov/business-guidance/blog/2024/04/updated-ftc-health-breach-notification-rule-puts-new-provisions-place-protect-users-health-apps

Federal Trade Commission Protects Consumer Information

- The Federal Trade Commission (FTC) is a federal agency and has the authority to investigate “organizations, business, conduct, practices and management of any person, partnership, or corporation engaged in or whose business affects commerce.”
- FTC Act/Rules protect consumers if businesses commit fraud or deceive them
- Due to concerns consumers may suffer identity theft or information otherwise exploited, the FTC regulates how businesses use consumer information
- An organization that fails to protect a consumer’s information, misuses it or discloses it, may violate the Federal Trade Commission Act which prohibits organizations from unfair or deceptive acts and practices in or affecting commerce.

1) FTC Authority:https://www.ftc.gov/about-ftc/mission/enforcement-authority

FTC Amended Health Breach Notification Rule (HNBR)

April 26, 2024 - HNBR Amendment

Applies to both health apps and similar technologies not covered by HIPAA

- Modified definition of “Personal Health Record (PHR) identifiable health information” and added definitions for “covered health care provider” and “health care services or supplies.”
- Definition of “breach security” includes both data security breaches and unauthorized disclosures
  - “A breach of security includes **an unauthorized acquisition of unsecured PHR identifiable health information** in a personal health record that occurs as a result of a data breach or an unauthorized disclosure.”

FTC Amended HBNR Rule – Definition Updates

- PHR-related entity
  - Revised definition establishes that the Rule applies to entities that offer products and services through online services of vendors of personal health records, including mobile applications.
  - Updates “accesses information” to read “accesses unsecured PHR identifiable information.”
  - Updates the phrase “Web sites” to read “websites, *including any online service*.”
- The technical capacity to draw information from multiple sources matters in the definition of “Personal Health Record”

FTC Amended HBNR – Breach Notice

- Expands the use of electronic notice to consumers
  - New focus: email in combination with other forms of electronic notice like text messages or in-app messaging
- Notices to consumers must include more information and must be “clear and conspicuous” and “reasonably understandable.”
  - Identity of any third parties that acquired unsecured PHR identifiable information
  - Describe the types of health information the breach involved

FTC Amended HBNR – Breach Notice (continued)

- Covered entities must move quickly to notify consumers and the FTC regarding breaches involving **500 or more people**
  - Must notify the FTC at the same time notices to affected individuals are sent
    - Without unreasonable delay and in no case later than 60 calendar days after discovery
- For breaches involving **fewer than 500 people**, covered entities must notify the FTC annually and no later than 60 calendar days following the end of the year
  - Notice to affected individuals must still occur without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach of security

FTC Recent Settlements

FTC Enforcement Action to Bar GoodRx from Sharing Consumers' Sensitive Health Info for Advertising

Under proposed order, GoodRx will pay a $1.5 million civil penalty for failing to report its unauthorized disclosure of consumer health data to Facebook, Google, and other companies

"We will vigorously enforce the Health Breach Notification Rule to defend consumer's health data from exploitation. Companies collecting this information should be aware that the FTC will not tolerate health privacy abuses."

- Samuel Levine, Director of the FTC's Bureau of Consumer Protection

"The FTC is serving notice that it will use all of its legal authority to protect American consumers' sensitive data from misuse and illegal exploitation."

- Samuel Levine, Director of the FTC's Bureau of Consumer Protection

Ovulation Tracking App Premom Will be Barred from Sharing Health Data for Advertising Under Proposed FTC Order

FTC says company disclosed user health data to third parties, deceived users about its data sharing practices and violated Health Breach Notification Rule

1) https://www.ftc.gov/news-events/news/press-releases/2023/05/ovulation-tracking-app-premom-will-be-barred-sharing-health-data-advertising-under-proposed-ftc

https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising

Violations

- Treated as a violation of the rule under section 18 of the Federal Trade Commission Act regarding unfair or deceptive acts or practices
- Penalties:
  - Civil Penalties up to $51,744 per violation of HBNR
  - Criminal – referred to U.S. Department of Justice for prosecution

On the Horizon

How Can We Help?

Karin Anderson
Principal
kanderson@pyapc.com

Erin Walker
Manager
ewalker@pyapc.com

pyapc.com
800.270.9629