Health Privacy + Security Law Workshop: New Developments

2023 Privacy+Security Forum Spring Academy

Adam Greene, Davis Wright Tremaine LLP

Agenda

- Healthcare Website Disclosures and Recent OCR Guidance
- Health Information Privacy in the Wake of *Dobbs*
- Status of HIPAA Rulemaking
- Changes to 42 C.F.R. Part 2
- 30-Minute Break
- Update on Information Blocking
- FTC Developments with Respect to Health and Wellness Apps
- State Privacy Laws
- Health Information Enforcement Actions

Healthcare Website Disclosures and Recent OCR Guidance


DO YOU
KNOW
10PM
WHERE YOUR
CHILDREN ARE?
WHAT YOUR MARKETING
DEPARTMENT IS DOING?

2019 Class Action Complaint

- “For example, a patient exchanging communications with Defendant relating to “sexually transmitted diseases” would have the following information disclosed by Defendant to [3rd Party 1], [3rd Party 2], and [3rd Party 3]:
  - The exact contents of the communication that the patient caused to be sent to the Defendant. In this case, a GET request2 that consists of the following data: "diseases-conditions/sexually-transmitted-disease; and
  - Data elements that are personally identifiable information, including Internet cookies, the patient's IP address, unique device identifiers, and a browser-fingerprint, all of which connect the contents of the communication to the patient.”

Mass General Brigham, Dana-Farber to pay $18.4M settlement over privacy allegations

Jan 6, 2022, 3:30pm EST

In the original lawsuit, the anonymous patients said both Mass General Brigham and Dana-Farber websites codes had employed tools to collect data on potential and ongoing patients. The hospitals used these tools to allegedly disclose information to [3rd Party 1], [3rd Party 2], [3rd Party 3], [3rd Party 4], [3rd Party 5], [3rd Party 6], and [3rd Party 7], including search history tied to a patient's Internet Protocol address; logins to patient portals; creation of an appointment request; and communications about providers, treatments, conditions and bill payment.

Boston Business Journal

https://www.bizjournals.com/boston/news/2022/01/06/mass-general-brigham-dana-farber-to-pay-184m-se.html


HHS.gov
U.S. Department of Health & Human Services
Health Information Privacy
I'm looking for...
A-Z Index
HIPAA for Individuals
Filing a Complaint
HIPAA for Professionals
Newsroom
HHS > HIPAA Home > For Professionals > Privacy > Guidance Materials > Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates
HIPAA for Professionals
Regulatory Initiatives
Privacy
Summary of the Privacy Rule
Guidance
Combined Text of All Rules
HIPAA Related Links
Text Resize A A A
Print
Share
Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates
The Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) is issuing this Bulletin to highlight the obligations of Health Insurance Portability and Accountability Act of 1996 (HIPAA) covered entities[1] and business associates[2] ("regulated entities") under the HIPAA Privacy, Security, and Breach Notification Rules ("HIPAA Rules") when using online tracking technologies ("tracking technologies").[3] OCR administers and enforces the HIPAA Rules, including by investigating breach reports and complaints about regulated entities' noncompliance with the HIPAA Rules. A regulated entity's failure to comply with the HIPAA Rules may result in a civil money penalty.[4]

Websites and PHI

- Is website tracking information individually identifiable?
  - Email address
  - IP address
  - Unique identifier in cookie or login

Websites and PHI

- Is website tracking information Health Information?
  - According to guidance, yes if:
    - Authenticated page limited to patients/members
    - Unauthenticated page but reveals:
      - Login
      - Scheduling an appointment
      - Search for a doctor
      - Specific condition or treatment
  - According to guidance, no if only identifies that someone visited home page/non-condition specific page and does not reveal health-related actions

Next Steps

- Identify all information collected about website visitors.
- Categorize as PHI or personal information (PI) based on whether it is related to health care (e.g., identifies visitor as a patient/member).
- For PHI, (1) ensure that all uses and disclosures are for permissible purposes under HIPAA and (2) business associate agreements are in place with third party service providers.
- For PI, (1) ensure compliance with online privacy policy and (2) analyze whether state privacy laws apply.

Health Information Privacy in the Wake of *Dobbs*

Syllabus

NOTE: Where it is feasible, a syllabus (headnote) will be released, as is being done in connection with this case, at the time the opinion is issued. The syllabus constitutes no part of the opinion of the Court but has been prepared by the Reporter of Decisions for the convenience of the reader. See *United States* v. *Detroit Timber & Lumber Co.*, 200 U. S. 321, 337.

SUPREME COURT OF THE UNITED STATES

Syllabus

DOBBS, STATE HEALTH OFFICER OF THE MISSISSIPPI DEPARTMENT OF HEALTH, ET AL. *v.* JACKSON WOMEN'S HEALTH ORGANIZATION ET AL.

CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE FIFTH CIRCUIT

No. 19–1392. Argued December 1, 2021—Decided June 24, 2022

Mississippi's Gestational Age Act provides that "[e]xcept in a medical

Potential HIPAA Permissions for Disclosures of Reproductive Health Information

- When required by law. [45 C.F.R. § 164.512(a)]
- In response to a court order. [45 C.F.R. § 164.512(e)]
- To law enforcement pursuant to a court order, court-ordered warrant, subpoena issued by a judicial officer, grand jury subpoena, or administrative request that includes three elements. [45 C.F.R. § 164.512(f)(1)]
- To report a crime on the premises. [45 C.F.R. § 164.512(f)(6)]
- To avert a serious and imminent threat to the health or safety of a person. [45 C.F.R. § 164.512(j)]
- Workforce member believes in good faith that the covered entity has engaged in unlawful conduct. [45 C.F.R. § 164.502(j)]

FOR IMMEDIATE RELEASE
June 29, 2022

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

HHS Issues Guidance to Protect Patient Privacy in Wake of Supreme Court Decision on Roe

Guidance includes information about what's protected – and what's not – when using period trackers and other health information apps on smartphones.

On the heels of the Supreme Court ruling in *Dobbs vs. Jackson Women's Health Organization*, where the right to safe and legal abortion was taken away, President Biden and U.S. Department of Health and Human Services (HHS) Secretary Xavier Becerra called on HHS agencies to take action to protect access to sexual and reproductive health care, including abortion, pregnancy complications, and other related care. Today, in direct response, the HHS Office for Civil Rights (OCR) issued new guidance to help protect patients seeking reproductive health care, as well as their providers.

OCR Guidance

- “The Privacy Rule permits but **does not require** covered entities to disclose PHI about an individual, without the individual’s authorization, when such disclosure is required by another law and the disclosure complies with the requirements of the other law.”
- “In the absence of a mandate enforceable in a court of law, the Privacy Rule’s permission to disclose PHI for law enforcement purposes does not permit a disclosure to law enforcement where a hospital or other health care provider’s workforce member chose to report an individual’s abortion or other reproductive health care.”
- “A statement indicating an individual’s intent to get a legal abortion, or any other care tied to pregnancy loss, ectopic pregnancy, or other complications related to or involving a pregnancy does not qualify as a ‘serious and imminent threat to the health or safety of a person or the public’.”

Senators Seek HIPAA Changes to Protect Reproductive Info

Letter Sent to HHS Secretary Urges 'Immediate Action' for HIPAA Rule-Making

Marianne Kolbasuk McGee (HealthInfoSec) • September 15, 2022

Twitter Facebook LinkedIn Credit Eligible Get Permission

https://www.healthcareinfosecurity.com/senators-seek-hipaa-changes-to-protect-reproductive-info-a-20086

Texas H.B. 1280

This Act may be cited as the Human Life Protection Act of 2021.

* * * * *

Sec. 170A.002. PROHIBITED ABORTION; EXCEPTIONS. (a) A person may not knowingly perform, induce, or attempt an abortion.

* * * * *

Sec. 170A.004. CRIMINAL OFFENSE. (a) A person who violates Section 170A.002 commits an offense.

(b) An offense under this section is a felony of the second degree, except that the offense is a felony of the first degree if an unborn child dies as a result of the offense.

Tex. Pen. Code Sec. 12.32. FIRST DEGREE FELONY PUNISHMENT. (a) An individual adjudged guilty of a felony of the first degree shall be punished by imprisonment in the Texas Department of Criminal Justice for life or for any term of not more than 99 years or less than 5 years.

NATIONAL

A Nebraska woman is charged with helping her daughter have an abortion

August 10, 2022 · 10:23 AM ET

THE ASSOCIATED PRESS

Idaho governor signs 'abortion trafficking' bill into law

April 6, 2023

"When your medical record can be used as evidence of illegal behavior, there is an issue. … As long as drug use is illegal, then the medical record can serve to incriminate the user. Furthermore, because those who use illegal substances and who are dependent on alcohol may disclose while in treatment for substance use disorders illegal acts that disclosure has the potential to be used for self-incrimination. … It is illegal to use heroin; it is not illegal to have diabetes. It is illegal to use marijuana; it is not illegal to be depressed. It is illegal to use street methamphetamine; it is not illegal to have hypertension. It is illegal to use PCP; it is not illegal to be obese. … It may be inconvenient for the health care delivery system to ask a patient for permission to codify information that could incriminate them in a legal forum, but it is disingenuous for health care providers to ignore the risk of disclosure of such information to the medical record. Respect for the autonomy of our patients requires that we seek permission from them prior to opening a gate that we cannot control, but which has clear implications."

- Comment by H. Westley Clark, former Director of Center for Substance Abuse Treatment in the Substance Abuse and Mental Health Administration, commenting on S. Wakeman & P. Friedman, *Outdated Privacy Law Limits Effective Substance Use Disorder Treatment: The Case Against 42 CFR Part 2*, Health Affairs, March 1, 2017, https://www.healthaffairs.org/do/10.1377/forefront.20170301.058969/.

OCR NPRM to Support Reproductive Health Care Privacy

- General Prohibition:
  1. Where the use or disclosure is for a criminal, civil, or administrative investigation into or proceeding against any person in connection with seeking, obtaining, providing, or facilitating reproductive health care.
  2. To identify any person for the purpose of initiating an activity described at paragraph (a)(5)(iii)(A)(1) of this section.

OCR NPRM to Support Reproductive Health Care Privacy

Scope of Prohibition:

Seeking, obtaining, providing, or facilitating reproductive health care includes, but is not limited to, any of the following:

- Expressing interest in
- Inducing
- Using
- Performing
- Furnishing
- Paying for
- Disseminating information about
- Arranging
- Insuring
- Assisting, or
- Otherwise taking action to engage in reproductive health care; or
- Attempting any of the same

OCR NPRM to Support Reproductive Health Care Privacy

- Applicability of Prohibition:
  1. The relevant criminal, civil, or administrative investigation or proceeding is in connection with any person seeking, obtaining, providing, or facilitating reproductive health care:
     - Outside of the state where the investigation or proceeding is authorized; and
     - Where such health care is lawful in the state in which it is provided.

OCR NPRM to Support Reproductive Health Care Privacy

- Applicability of Prohibition:
  2. The relevant criminal, civil, or administrative investigation or proceeding is in connection with any person seeking, obtaining, providing, or facilitating reproductive health care that:
     - Is protected, required, or authorized by Federal law, regardless of the state in which such health care is provided.

OCR NPRM to Support Reproductive Health Care Privacy

- Applicability of Prohibition:
  3. The relevant criminal, civil, or administrative investigation or proceeding is in connection with any person seeking, obtaining, providing, or facilitating reproductive health care that:
     - Is provided in the state in which the investigation or proceeding is authorized; and
     - That is permitted by the law of that state.

OCR NPRM to Support Reproductive Health Care Privacy

- Attestation:
  - Requestor must attest that the use or disclosure is not for a prohibited purpose:
    1. For a criminal, civil, or administrative investigation into or proceeding against any person in connection with seeking, obtaining, providing, or facilitating reproductive health care.
    2. To identify any person for the purpose of initiating an above activity.
  - Applies to health oversight, judicial, law enforcement, or coroner/medical examiner requests.

OCR NPRM to Support Reproductive Health Care Privacy

- Attestation Content:
  - A description of the information requested that identifies the information in a specific fashion, including one of the following:
    - The name of any individual(s) whose PHI is sought, if practicable.
    - If including the name(s) of any individual(s) whose PHI is sought is not practicable, a description of the class of individuals whose PHI is sought.
  - The name or other specific identification of the person(s), or class of persons, who are requested to make the use or disclosure.
  - The name or other specific identification of the person(s), or class of persons, to whom the covered entity is to make the requested use or disclosure.
  - A clear statement that the use or disclosure is not for a purpose prohibited under § 164.502(a)(5)(iii).
  - Signature of the person requesting the PHI, which may be an electronic signature, and date. If the attestation is signed by a representative of the person requesting the information, a description of such representative's authority to act for the person must also be provided.

OCR NPRM to Support Reproductive Health Care Privacy

- Defective Attestation:
  - The attestation lacks a required element or statement.
  - The attestation contains an element or statement not required by paragraph (c) of this section.
  - The attestation is a compound attestation.
  - The covered entity has actual knowledge that material information in the attestation is false.
  - It is objectively unreasonable for the covered entity to believe that the attestation is true with respect to the statement that it is not for a prohibited purpose.

OCR NPRM to Support Reproductive Health Care Privacy

- Attestations
  - Lying on an attestation could be a HIPAA criminal violation (obtaining PHI in violation of HIPAA).
  - Disclosing without an attestation or based on a defective authorization could be reportable breach.

OCR NPRM to Support Reproductive Health Care Privacy

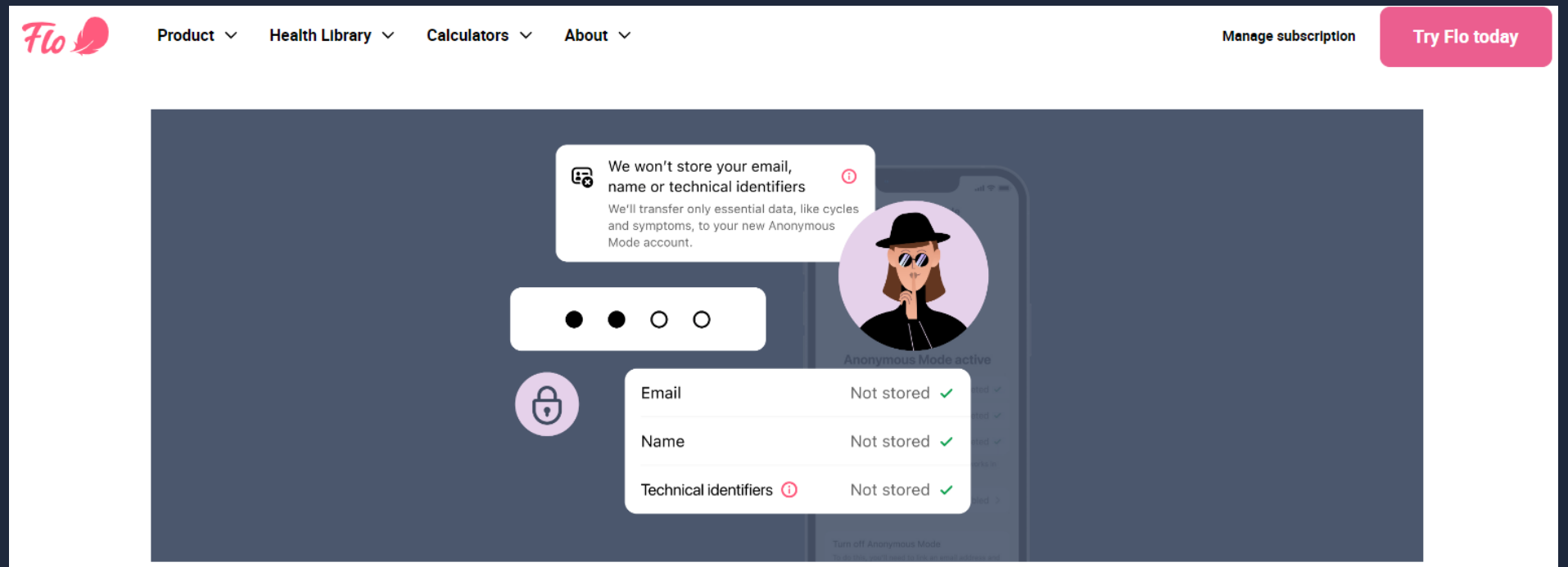
- Notice of Privacy Practices
  - Description of prohibition with at least one example
  - Description of the types of uses and disclosures for which attestation is required (e.g., health oversight, judicial, law enforcement, and coroner/medical examiner)
- Law Enforcement
  - Permissible disclosures for law enforcement administrative requests would only be if “response is required by law.”

Google Changes Location History Practices

Location History is a Google account setting that is off by default, and for those that turn it on, we provide simple controls like auto-delete so users can easily delete parts, or all, of their data at any time. Some of the places people visit — including medical facilities like counseling centers, domestic violence shelters, abortion clinics, fertility centers, addiction treatment facilities, weight loss clinics, cosmetic surgery clinics, and others — can be particularly personal. Today, we're announcing that if our systems identify that someone has visited one of these places, we will delete these entries from Location History soon after they visit. This change will take effect in the coming weeks.

- Jen Fitzpatrick, Senior Vice President, Google, https://blog.google/technology/safety-security/protecting-peoples-privacy-on-health-topics/ (July 1, 2022)

Flo Health Enables Anonymous Mode



Flo 'Anonymous Mode' Now Live, Offering Significant Advancement in the Privacy and Security of Reproductive Health Data

New State Protections

Cal. Civ. Code § 56.108 (.

- "[A] provider of health care … shall not release medical information related to an individual seeking or obtaining an abortion in response to a subpoena or request if that subpoena or request is based on either another state's laws that interfere with a person's rights under the Reproductive Privacy Act (Article 2.5 (commencing with Section 123460) of Chapter 2 of Part 2 of Division 106 of the Health and Safety Code) or a foreign penal civil action, as defined in Section 2029.200 of the Code of Civil Procedure."
- "A provider of health care … shall not release medical information that would identify an individual or that is related to an individual seeking or obtaining an abortion to law enforcement for either of the following purposes, unless that release is pursuant to a subpoena not otherwise prohibited by subdivision (a):
    1. Enforcement of another state's law that would interfere with a person's rights under the Reproductive Privacy Act (Article 2.5 (commencing with Section 123460) of Chapter 2 of Part 2 of Division 106 of the Health and Safety Code).
    2. Enforcement of a foreign penal civil action, as defined in Section 2029.200 of the Code of Civil Procedure."

Status of HIPAA Rulemaking

2021 NPRM: Right of Access

- 30 days + 30 days becomes “as soon as practicable” + 15 calendar days + 15 calendar days
- Policy must prioritize “urgent or otherwise high priority requests”
- Third-party directives: (1) limited to e-copy of EHR; and (2) can be based on verbal request
- Clarifies right of inspection and “unreasonable measures”

2021 NPRM: Right of Access

- Right to receive copy through a “personal health application”
- Must post fees and provide individualized estimate upon request
- Right to have a covered entity submit an access request to a health care provider on individual’s behalf

2021 NPRM: Notice of Privacy Practices

- Ends requirement to obtain acknowledgment of receipt
- Substantially increases required language
- Adds right to discuss the notice with designated contact person

2021 NPRM: Other Proposals

- Clarifies definition of “health care operations”
- Adds exception to minimum necessary standard for case management and care coordination
- Permits disclosure for treatment to social services agencies, community-based organizations, home and community-based providers, and similar third parties
- Revises “professional judgment” to “good faith belief”
- “Serious and imminent threat” → “serious and reasonably foreseeable threat”

April 2022 Request for Information

- With respect to penalties and audits, “the Secretary shall consider whether the covered entity or business associate has adequately demonstrated that it had, for not less than the previous 12 months, recognized security practices in place ….”
  - Questions about “recognized security practices” that organizations have implemented.
  - What steps do organizations take to ensure that recognized security practices are in place and consistently in use?

April 2022 Request for Information

- Distribution of penalties/settlements to harmed individuals
  - What constitutes compensable harm?
  - Should harm be presumed in certain cases? If not, what evidence of harm is needed?
  - Should there be a minimum or maximum percentage distributed to harmed individuals?
  - How should harmed individuals be identified and notified?
- Deadline for comments: June 6, 2022

Status

Rule	Last Action	Next Action
Reproductive Health Care NPRM	NPRM published 4/17/23	Comments due 6/16/23
42 C.F.R. Part 2	NPRM published 12/2/22, comment period ended 1/31/23	Final rule (Late 2023?)
2021 Coordinated Care NPRM	NPRM published 1/21/21, comment period ended 5/6/21	Final rule (2024?)
April 2022 RFI on Distribution of Penalties and Recognized Security Practices	Comments due 6/6/22	NPRM (?)

Changes to 42 C.F.R. Part 2

CARES Act

- Patient can provide general treatment, payment, health care operations ("TPO") consent.
- Once disclosed for TPO, then Part 2 record may be redisclosed consistent with HIPAA.
- HIPAA penalties apply to the Part 2 Rule.
- New breach notification requirement consistent with HIPAA.
- Waiting on regulations.

SAMHSA
Substance Abuse and Mental Health Services Administration

Home | Site Map | Contact Us

Search SAMHSA.gov Search

Find Treatment | Practitioner Training | Public Messages | Grants | Data | Programs | Newsroom | About Us | Publications

Home » Newsroom » Statements

Newsroom

- Coronavirus (COVID-19)
- SAMHSA Blog
- Media Guidelines for Bullying Prevention
- Press Announcements
- Statements
- Logo Use Guidelines

Statement on 42 CFR Part 2 Amendments Process

Friday, April 9, 2021

SAMHSA is working with the HHS Office for Civil Rights on a Notice of Proposed Rulemaking to address the changes required by the CARES Act, to the 42 CFR part 2 regulations governing the confidentiality of substance use disorder patient records. We intend to publish these amendments later this year in the Federal Register, and we will be seeking comments from the public. Until new regulations are promulgated, the current 42 CFR part 2 regulations remain in effect. We know that many stakeholders are eagerly awaiting these revisions and appreciate your patience as we work to provide a thoughtful and thorough review of these provisions and amendments.

Last Updated: 04/09/2021

December 2022 Proposed Rule

- Revises 42 C.F.R. Part 2 (“Part 2 Rule”) terms to be more consistent with HIPAA (e.g., “use and disclosure” throughout)
- Revises Part 2 Rule’s consent requirement to make more consistent with HIPAA
- Permits patient to authorize uses and disclosures of Part 2 Records for treatment, payment, and health care operations (“TPO”)
- Recipient of Part 2 Records based on TPO consent can further use and disclose as permitted under HIPAA

45

December 2022 Proposed Rule

- Patient right to an accounting of disclosures
- Applies HIPAA Breach Notification Rule to Part 2 Rule
- Applies HIPAA criminal and civil enforcement mechanisms to Part 2 Rule
- Prohibits use or disclosure of Part 2 Records for civil, criminal, administrative, or legislative proceeding against the patient

46

December 2022 Proposed Rule

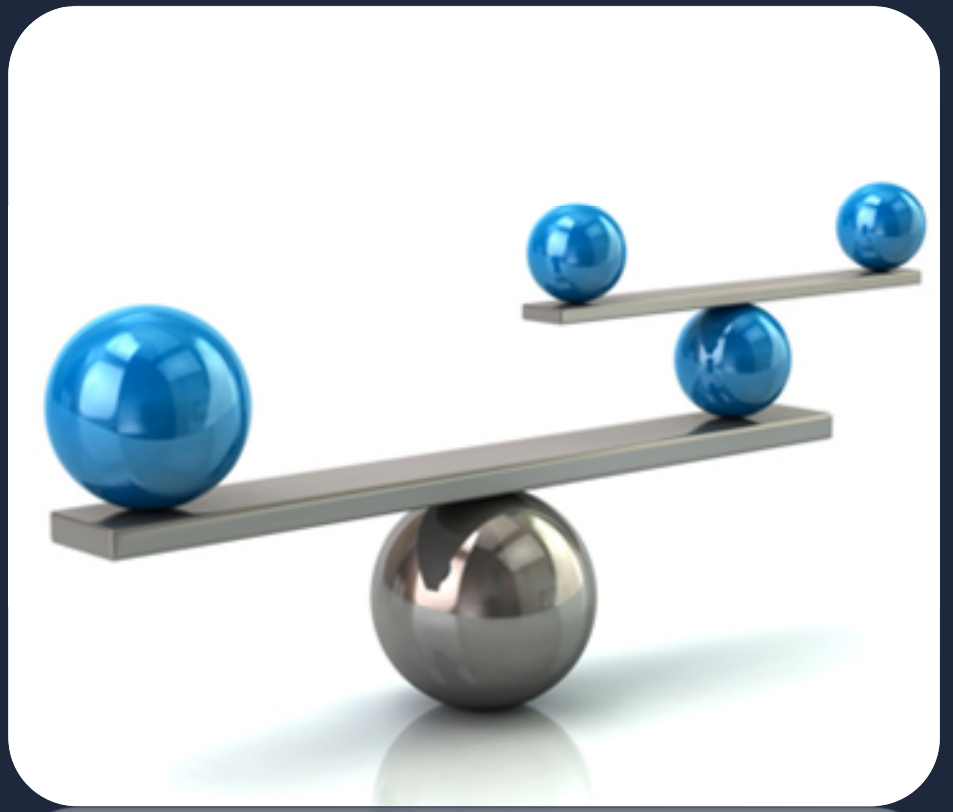
- Wolf in Sheep's Clothing?
  - Continued need to segregate data
  - Limitations with health IT
  - Increased transparency of violations due to breach notification
  - Increased risk of enforcement

30-Minute Break

Update on Information Blocking

Cures Act – Information Blocking Definition

- Except if:
  - Practice is required by law
  - Falls under HHS rulemaking exception
- Practice is likely to …
- Interfere with, prevent, or materially discourage …



Cures Act – Information Blocking Definition (Cont'd)

- Access, exchange, or use …
- Electronic Health Information
- Knowledge
  - Knows or Should Know (health information technology developer, exchange, or network); or
  - Knows practice is unreasonable (health care provider)

Information Blocking - Actors

Health Care Providers

Health IT Developers of Certified Health IT

Health Information Networks/Health Information Exchanges

Eight Exceptions

HHS Office of the National Coordinator of Health IT, https://www.healthit.gov/topic/information-blocking

Guidance:

“To further illustrate, it also would likely be considered an interference:

- where a delay in providing access, exchange, or use occurs after a patient logs in to a patient portal to access EHI that a health care provider has (including, for example, lab results) and such EHI is not available—for any period of time—through the portal.”

https://www.healthit.gov/curesrule/resources/information-blocking-faqs

Can I Block EHI from Going to the Patient Portal If I Believe Doing So Is Reasonable?

- Statute:
  - “In this section, the term ‘information blocking’ means a practice that … if conducted by a health care provider, such provider knows that such practice is unreasonable ….”
- Regulation:
  - “Information blocking means a practice that … If conducted by a health care provider, such provider knows that such practice is unreasonable …”
- Risk – HHS may take the position that anything that does not fall within a regulatory exception is inherently unreasonable.

Status of Enforcement

- Applicability date was April 5, 2021
- OIG enforcement with respect to health IT developers and HIEs/HINs:
  - $1 million per violation
  - Proposed enforcement rule on 4/24/20
  - Final rule expected shortly
  - Enforcement will begin for conduct occurring 60 days after final rule

Current Status of Final OIG Rule

OFFICE of INFORMATION and REGULATORY AFFAIRS
OFFICE of MANAGEMENT and BUDGET
EXECUTIVE OFFICE OF THE PRESIDENT

Reginfo.gov

U.S. General Services Administration

Search: Agenda Reg Review ICR

Go

Home | Unified Agenda | Regulatory Review | Information Collection Review | FAQs / Resources | Contact Us

Pending EO 12866 Regulatory Review

RIN: 0936-AA09 **View EO 12866 Meetings**

Received Date: 04/07/2023

Title: Amendments to Civil Monetary Penalty Law Regarding Grants, Contracts, and Information Blocking

Agency/Subagency: HHS / OIG

Stage: Final Rule

Legal Deadline: None

Section 3(f)(1) Significant: No

International Impacts: No

Affordable Care Act [Pub. L. 111-148 & 111-152]: No

Pandemic Response: No

Dodd-Frank Wall Street Reform and Consumer Protection Act, [Pub. L. 111-203]: No

Status of Enforcement

- Enforcement with respect to health care providers:
  - No proposed enforcement rule yet
  - No information on what “appropriate disincentives will be”
  - No information on which agency will enforce the rule
  - No information on whether conduct prior to final enforcement rule is subject to enforcement

FTC Developments with Respect to Health and Wellness Apps

FTC & Health Apps

- Section 5 of the FTC Act prohibits unfair and deceptive trade practices
- FTC Health Breach Notification Rule governing personal health records

FTC & Health Apps

- FTC Health Breach Notification Rule Request for Public Comment (5/22/20)
- Three members of Congress urge FTC to take action against menstruation-tracking mobile apps that violate the Health Breach Notification Rule (3/4/21).
- FTC enters into consent order with Flo Health over disclosures from menstruation app to Facebook, Flurry, Fabric, and Google (6/22/21).
- FTC issues Policy Statement “clarifying” the Health Breach Notification Rule’s application to health and fitness apps (9/15/21).

FTC & Health Apps

- PHR Identifiable Health Information:
  - Individually Identifiable Health Information
    - Definition limited to information created or received by a health care provider, health plan, employer, or health care clearinghouse
  - That is provided by or on behalf of the individual
  - That identifies the individual

FTC & Health Apps

- Personal Health Record:
  - Electronic record
  - PHR identifiable health information
  - Can be drawn from multiple sources
  - Managed, shared, and controlled by or primarily for the individual

FTC & Health Apps

“Under the definitions cross-referenced by the Rule, the developer of a health app or connected device is a ‘health care provider’ because it ‘furnish[es] health care services or supplies.’”

FTC Statement on Breaches by Health Apps and Other Connected Devices

FTC & Health Apps

“The statute directing the FTC to promulgate the Rule requires that a “personal health record” be an electronic record that can be drawn from multiple sources. The Commission considers apps covered by the Rule if they are capable of drawing information from multiple sources, such as through a combination of consumer inputs and application programming interfaces (‘APIs’).”

FTC Statement on Breaches by Health Apps and Other Connected Devices

FTC & Health Apps

“For example, an app is covered 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.”

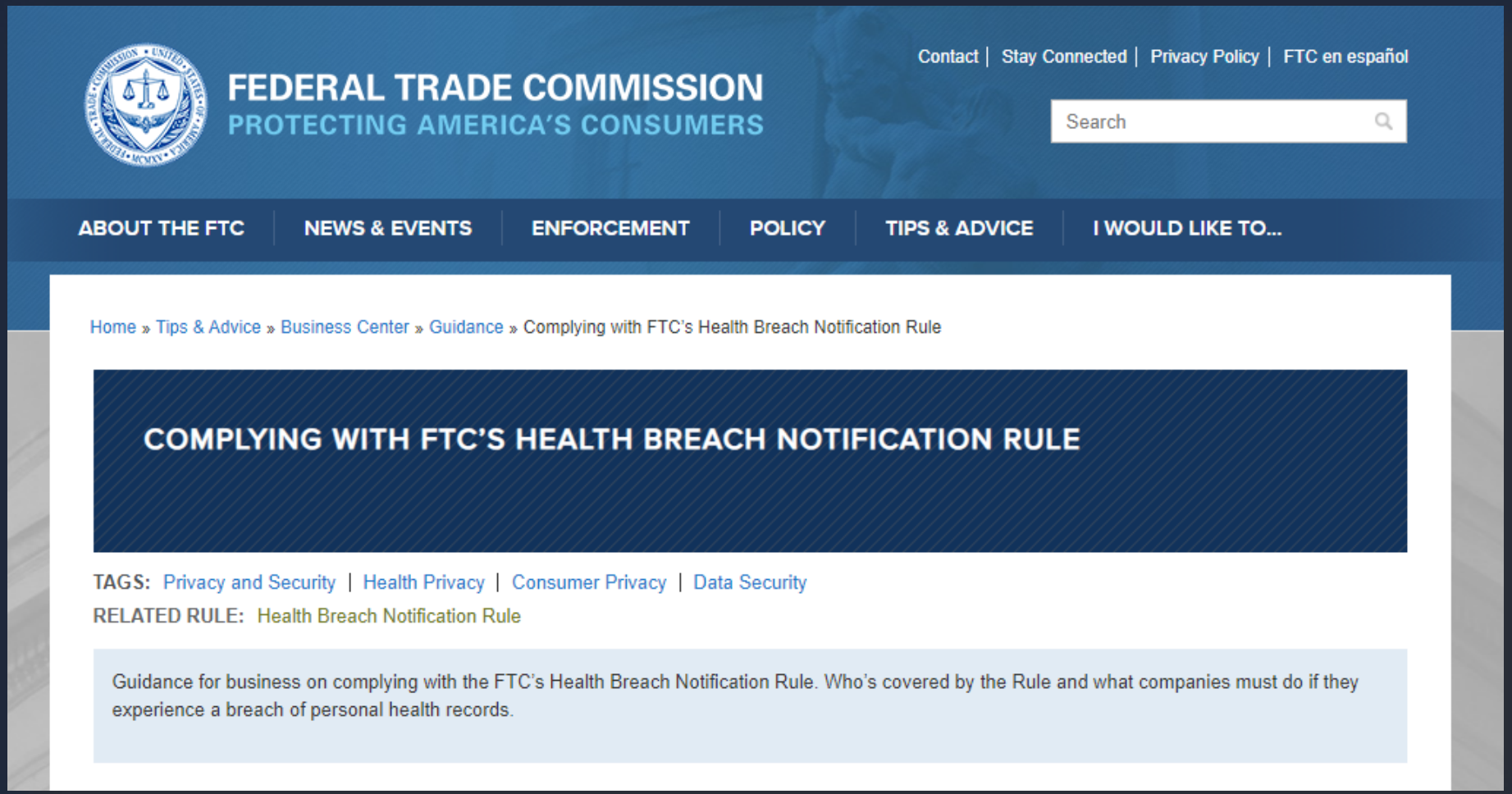
FTC Statement on Breaches by Health Apps and Other Connected Devices

FTC & Health Apps

“For example, if a blood sugar monitoring app draws health information only from one source (e.g., a consumer’s inputted blood sugar levels), but also takes non-health information from another source (e.g., dates from your phone’s calendar), it is covered under the Rule.”

FTC Statement on Breaches by Health Apps and Other Connected Devices

FTC Health Breach Notification Rule Resources (Jan. 2022)



In the Matter of GoodRx

“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”

- Feb. 1, 2023

In the Matter of GoodRx

- “GoodRx has promised its users that it would share their personal information, including their personal health information, with limited third parties and only for limited purposes; that it would restrict third parties’ use of such information; and that it would never share personal health information with advertisers or other third parties.”
- “In one campaign, which GoodRx ran in August 2019, GoodRx compiled lists of its users who had purchased particular medications, uploaded their email addresses, phone numbers, and mobile advertising IDs to Facebook to identify their profiles, and labeled them by the medication they had purchased. GoodRx then targeted these users with health-related advertisements.”

In the Matter of GoodRx

- "GoodRx's repeated, unauthorized disclosures of users' personal and health information over the course of a four-year period have revealed extremely intimate and sensitive details about GoodRx users that could be linked to (or used to infer information about) chronic physical or mental health conditions, medical treatments and treatment choices, life expectancy, disability status, information relating to parental status, substance addiction, sexual and reproductive health, sexual orientation, and other highly sensitive and personal information."
- "These actions are deceptive or unfair acts, in violation of Section 5 of the FTC Act, 15 U.S.C. § 45(a), and violate the Health Breach Notification Rule, 16 C.F.R. § 318."

In the Matter of GoodRx

“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”

- Feb. 1, 2023

In the Matter of GoodRx

"GoodRx's website and Mobile Apps are electronic records of PHR identifiable health information that are capable of drawing information from multiple sources, including inputs from users; Medication Purchase Data, pricing, and refill information from Pharmacy Benefit Managers; pharmacy information from pharmacies; information about prescribed medications from healthcare professionals (such as the name of a medication prescribed during a telehealth session); and users' geographic location information from a third-party vendor that approximates geolocation based on IP address. **The information is also managed, shared, or controlled by or primarily for the user.** GoodRx lets users keep track of their personal health information, including to save, track, and receive alerts about their prescriptions, refills, pricing, and medication purchase history."

In the Matter of BetterHelp

“FTC to Ban BetterHelp from Revealing Consumers’ Data, Including Sensitive Mental Health Information, to Facebook and Others for Targeted Advertising”

“BetterHelp will be required to pay $7.8 million for deceiving consumers after promising to keep sensitive personal data private, agency says”

- Mar. 2, 2023

In the Matter of BetterHelp

“From 2013 to December 2020, however, Respondent continually broke these privacy promises, monetizing consumers’ health information to target them and others with advertisements for the Service. For example, from 2018 to 2020, Respondent used these consumers’ email addresses and the fact that they had previously been in therapy to instruct Facebook to identify similar consumers and target them with advertisements for the Service, bringing in tens of thousands of new paying users, and millions of dollars in revenue, as a result.”

State Privacy Laws

States with General Privacy Laws

State	Threshold*	PHI Exempt	CE/BA Exempt	Non-Profits	Date
California	$25M or 100,000 CA residents	Yes (in hands of CE/BA)	No	Generally no	Current
Colorado	100,000 CO residents	Yes (in hands of CE/BA)	No	Yes	July 1, 2023
Connecticut	100,000 CT residents	Yes	Yes	No	July 1, 2023
Iowa	100,000 IA residents	Yes	No	No	Jan. 1, 2025
Indiana	100,000 IN residents	Yes	Yes	No	
Utah	$25M and 100,000 UT residents	Yes	Yes	No	Dec. 31, 2023
Virginia	100,000 VA residents	Yes	Yes	No	Current

* Does not include alternative thresholds based on % of revenue from sale of personal information.

Washington My Health My Data Act

- Covers “consumer health data” (CHD), which is broadly defined but excludes PHI.
- Covers WA residents and non-WA residents whose information is bought, rented, accessed, retained, received, acquired, inferred, derived, or otherwise processed in WA.
- Private right of action but must prove damages.

Washington My Health My Data Act

- ***Transparency***. Posting of consumer health data privacy policy.
- ***Consent*. Obtain consent to collect or share CHD (other than as necessary to provide product or service).**
- ***Authorization for Sale.*** More detailed authorization for sale of CHD, including name and contact info of purchasers.
- ***Geofencing Restriction***. Restrict on geofencing around health care entities.

Washington My Health My Data Act

- ***Consumer Rights***.
  - Confirmation of collection, sharing, or selling CHD.
  - Access to CHD and list of third parties and affiliated with whom CHD was shared or sold.
  - Right to withdraw consent.
  - Right of deletion.
- ***Security Obligations***. Reasonable security practices to protect confidentiality, integrity, and accessibility.

State Law Issues

- Is website visitor information subject to HIPAA, state law, or both?
- Does the state's breach notification law apply to health information? Is there special treatment of HIPAA entities?
- Employee privacy under California Consumer Privacy Act.

Health Information Enforcement Actions

OCR Aggregate Enforcement Data (Mar. 2023)

- Voluntary corrective action – 30,078 cases
- Technical assistance – 54,183 cases
- No violation – 14,408 cases
- Not eligible (e.g., no covered entity) – 218,092 complaints
- Financial enforcement – 130 cases
  - Highest action - $16 million (Anthem)
  - Average settlement/penalty - $1,037,144

42nd OCR Right of Access Case (Dec. 2022)

FOR IMMEDIATE RELEASE
December 15, 2022

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

HHS Civil Rights Office Resolves HIPAA Right of Access Investigation with $20,000 Settlement

Today, the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services announced a settlement with Health Specialists of Central Florida Inc., a provider in Florida that provides primary care, concerning a potential violation of the Health

Security Rule Enforcement

HHS Office for Civil Rights Settles HIPAA Investigation with Arizona Hospital System Following Cybersecurity Hacking

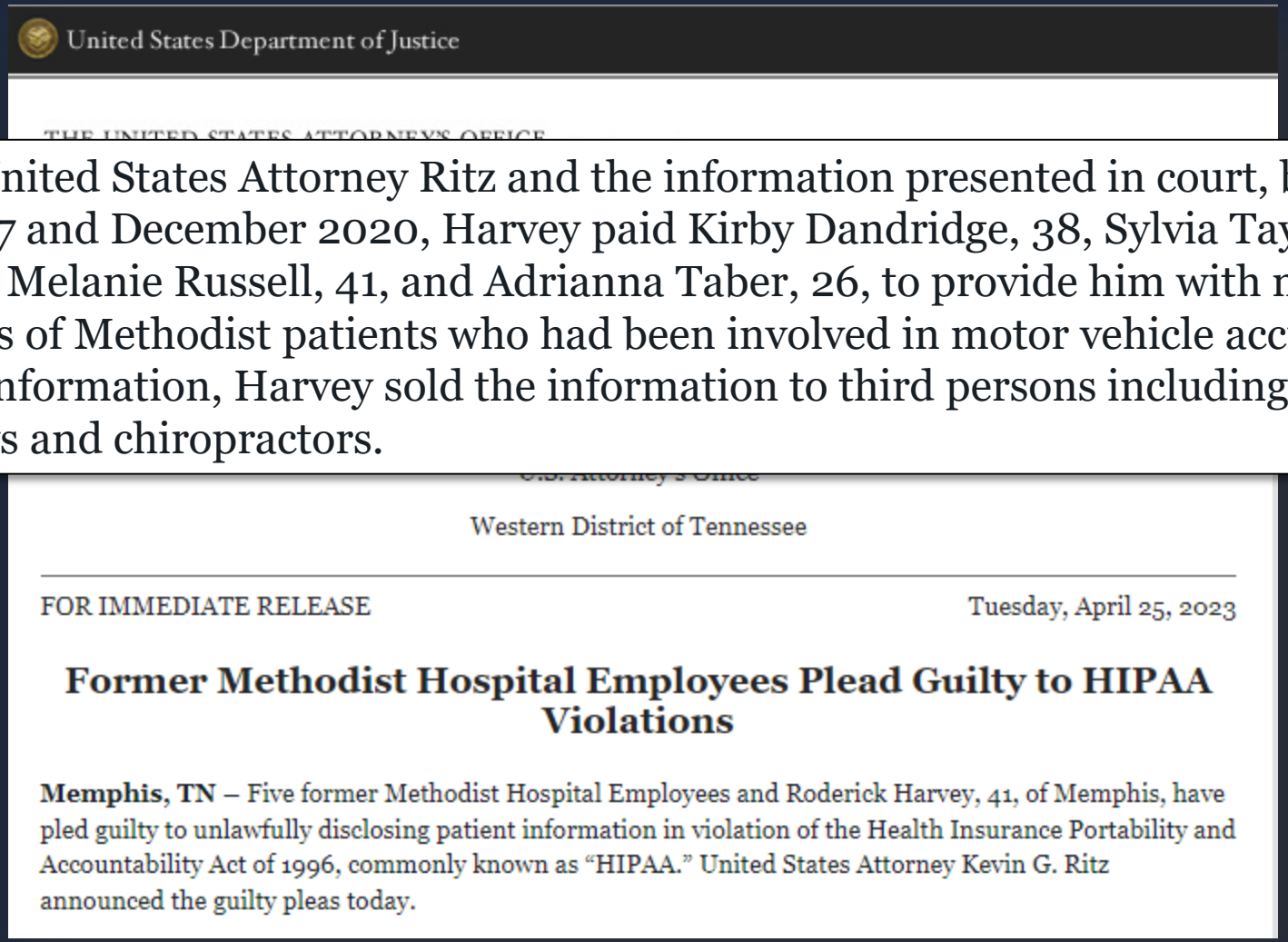
Banner Health pays $1.25 million to settle cybersecurity breach that affected nearly 3 million people

OCR has announced a settlement with Banner Health Affiliated Covered Entities ("Banner Health"), a nonprofit health system headquartered in Phoenix, Arizona, to resolve a data breach resulting from a hacking incident by a threat actor in 2016 which disclosed the protected health information of 2.81 million consumers. The potential violations specifically include: the lack of an analysis to determine risks and vulnerabilities to electronic protected health information across the organization, insufficient monitoring of its health information systems' activity to protect against a cyber-attack, failure to

https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/banner-health/index.html 1/3

HIPAA Criminal Prosecutions

According to United States Attorney Ritz and the information presented in court, between November 2017 and December 2020, Harvey paid Kirby Dandridge, 38, Sylvia Taylor, 43, Kara Thompson, 31, Melanie Russell, 41, and Adrianna Taber, 26, to provide him with names and phone numbers of Methodist patients who had been involved in motor vehicle accidents. After obtaining the information, Harvey sold the information to third persons including personal injury attorneys and chiropractors.



United States Department of Justice

Western District of Tennessee

FOR IMMEDIATE RELEASE

Tuesday, April 25, 2023

Former Methodist Hospital Employees Plead Guilty to HIPAA Violations

Memphis, TN – Five former Methodist Hospital Employees and Roderick Harvey, 41, of Memphis, have pled guilty to unlawfully disclosing patient information in violation of the Health Insurance Portability and Accountability Act of 1996, commonly known as "HIPAA." United States Attorney Kevin G. Ritz announced the guilty pleas today.

For more information …

Adam Greene

Partner, Washington, DC

Davis Wright Tremaine

adamgreene@dwt.com

P: 202.973.4213