New Developments in Health Information Privacy and Security Law

Privacy + Security Forum Spring Academy

May 8, 2025

Adam Greene, Davis Wright Tremaine, DC

Davis Wright Tremaine LLP

Agenda

- HIPAA Amendments to Further Safeguard Reproductive Health Care
- HIPAA Security Rule Notice of Proposed Rulemaking
- Website Disclosures of Health Information
- Confidentiality of Substance Use Disorder Patient Records amendments
- State Consumer Health Data Laws
- FTC Enforcement of Health Privacy

HIPAA Amendments to Further Safeguard Reproductive Health Care

Reproductive Health Care Amendments

- Final rule on April 26, 2024.
- Compliance deadline of December 23, 2024.
  - Delayed February 16, 2026, deadline for amending notice of privacy practices.
- On December 5, 2024, HHS Office for Civil Rights (OCR) announced that it was committed to enforcing the amendments.

Reproductive Health Care Amendments

- Prohibition on using or disclosing protected health information (PHI) to investigate or impose liability on seeking, obtaining, providing, or facilitating lawful reproductive health care.
- Attestation of permitted purpose for uses and disclosures for health oversight activities, judicial and administrative proceedings, law enforcement, and (for decedents) coroners and medical examiners.
- Changes to HIPAA notice of privacy practices.

Reproductive Health Care Amendments

Reproductive Health Care Amendments

- *Purl v. HHS* (N.D. Tex.)
  - Preliminary injunction against HHS enforcing the 2024 amendments against physician and her practice.
  - HHS alleges no standing.
- *Texas v. HHS* (N.D. Tex.)
- *Tenn. v. HHS* (E.D. Tenn.)
  - 3/13/25 brief – "HHS's new leadership is currently reviewing the Rule."
  - HHS alleges no standing.

Current Challenges with 2024 Amendments

- Require attestation for all requests or make determination that PHI is potentially related to reproductive health care?
- Require attestation for all requests or distinguish health oversight, judicial, law enforcement, coroners, and medical examiners?
- Requestors, including federal agencies, are refusing to sign attestations.

Potential Future

- OCR and state attorneys general (AGs) enforce the amendments.
- OCR silently does not enforce amendments (AGs can still enforce).
- HHS stops defending rule in court cases and lets courts vacate the amendments.
- OCR issues notice of enforcement discretion (AGs can still enforce).
- OCR withdraws amendments through notice-and-comment rulemaking.

HIPAA Security Rule Notice of Proposed Rulemaking

Security Rule NPRM

- Eliminates “addressable” implementation specifications – all would be required.
- More detailed requirements, such as inventory of technology assets, network map, patch management with 15-day deadline, 1-hour deadline for terminating employee access, etc.
- Requires encryption and multifactor authentication with very limited exceptions.
- Requires business associates to agree to 24-hour notification of activation of contingency plan.
- Requires dozens of actions to be done on an annual basis.

Security Rule NPRM

- Proposed on January 6, 2025.
- Comments due on March 7, 2025.
- 4,747 comments received.
- Finalization of the rule as proposed seems unlikely.

898 **Federal Register** / Vol. 90, No. 3 / Monday, January 6, 2025 / Proposed Rules

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office of the Secretary

45 CFR Parts 160 and 164

RIN 0945–AA22

HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information

AGENCY: Office for Civil Rights (OCR), Office of the Secretary, Department of Health and Human Services.

ACTION: Notice of proposed rulemaking; notice of Tribal consultation.

SUMMARY: The Department of Health and Human Services (HHS or "Department") is issuing this notice of proposed rulemaking (NPRM) to solicit comment on its proposal to modify the Security Standards for the Protection of Electronic Protected Health Information ("Security Rule") under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act). The proposed modifications would revise existing standards to better protect the confidentiality, integrity, and availability of electronic protected health information (ePHI). The proposals in this NPRM would increase the cybersecurity for ePHI by revising the Security Rule to address: changes in the environment in which health care is provided; significant increases in breaches and cyberattacks; common deficiencies the Office for Civil Rights has observed in investigations into Security Rule compliance by covered entities and their business associates (collectively, "regulated entities"); other cybersecurity guidelines, best practices, methodologies, procedures, and processes; and court decisions that affect enforcement of the Security Rule.

DATES:

Comments: Submit comments on or before March 7, 2025.

Meeting: Pursuant to Executive Order 13175, Consultation and Coordination with Indian Tribal Governments, the Department of Health and Human

ADDRESSES: You may submit comments, identified by RIN Number 0945–AA22, by any of the following methods. Please do not submit duplicate comments.

- *Federal eRulemaking Portal:* You may submit electronic comments at *https://www.regulations.gov* by searching for the Docket ID number HHS–OCR–0945–AA22. Follow the instructions at *https://www.regulations.gov* for submitting electronic comments. Attachments should be in Microsoft Word or Portable Document Format (PDF).
- *Regular, Express, or Overnight Mail:* You may mail written comments to the following address only: U.S. Department of Health and Human Services, Office for Civil Rights, Attention: HIPAA Security Rule NPRM, Hubert H. Humphrey Building, Room 509F, 200 Independence Avenue SW, Washington, DC 20201. Please allow sufficient time for mailed comments to be timely received in the event of delivery or security delays.

Please note that comments submitted by fax or email and those submitted after the comment period will not be accepted.

Inspection of Public Comments: All comments received by the accepted methods and due date specified above may be posted without change to content to *https://www.regulations.gov*, which may include personal information provided about the commenter, and such posting may occur after the closing of the comment period. However, the Department may redact certain non-substantive content from comments or attachments to comments before posting, including: threats, hate speech, profanity, sensitive health information, graphic images, promotional materials, copyrighted materials, or individually identifiable information about a third-party individual other than the commenter. In addition, comments or material designated as confidential or not to be disclosed to the public will not be accepted. Comments may be redacted or rejected as described above without notice to the commenter, and the Department will not consider in rulemaking any redacted or rejected

for Docket ID number HHS–OCR–0945–AA22.

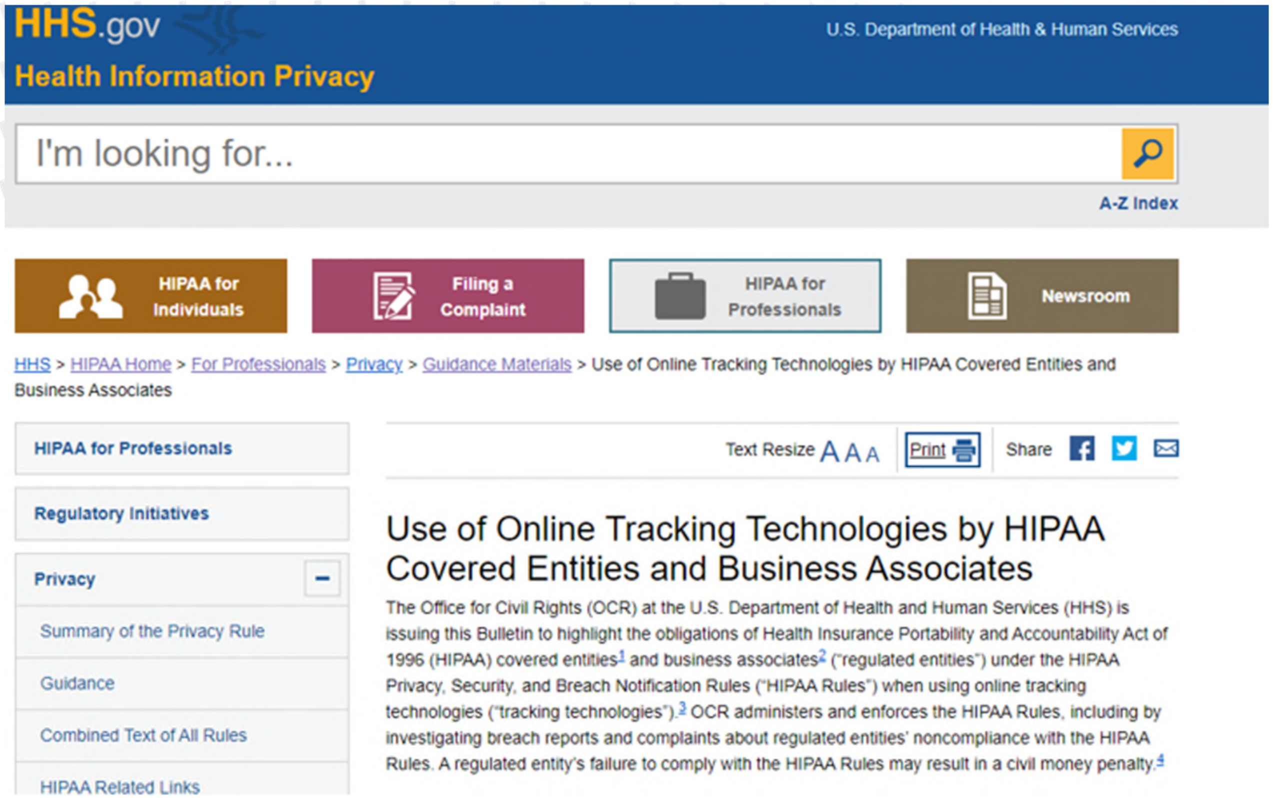
Tribal consultation meeting: To participate in the Tribal consultation meeting, you must register in advance at *https://hhsgov.zoomgov.com/meeting/register/vJItdOyhrjgoHxJWMDxozrxT98yXyCO3lks.*

FOR FURTHER INFORMATION CONTACT: Marissa Gordon-Nguyen at (202) 240–3110 or (800) 537–7697 (TDD), or by email at *OCRPrivacy@hhs.gov.*

SUPPLEMENTARY INFORMATION: The discussion below includes an Executive Summary, a description of relevant statutory and regulatory authority and history, the justification for this proposed regulation, a section-by-section description of the proposed modifications, and a regulatory impact analysis and other required regulatory analyses. The Department solicits public comment on all aspects of the proposed rule. The Department requests that persons commenting on the provisions of the proposed rule label their discussion of any particular provision or topic with a citation to the section of the proposed rule being addressed and identify the particular request for comment being addressed, if applicable.

Table of Contents

Website Disclosures



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

OCR and FTC Send Joint Letter to ~ 130 Health Care Providers

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
Office for Civil Rights

July 20, 2023

[Company]
[Address]
[City, State, Zip Code]
Attn: [Name of Recipient]

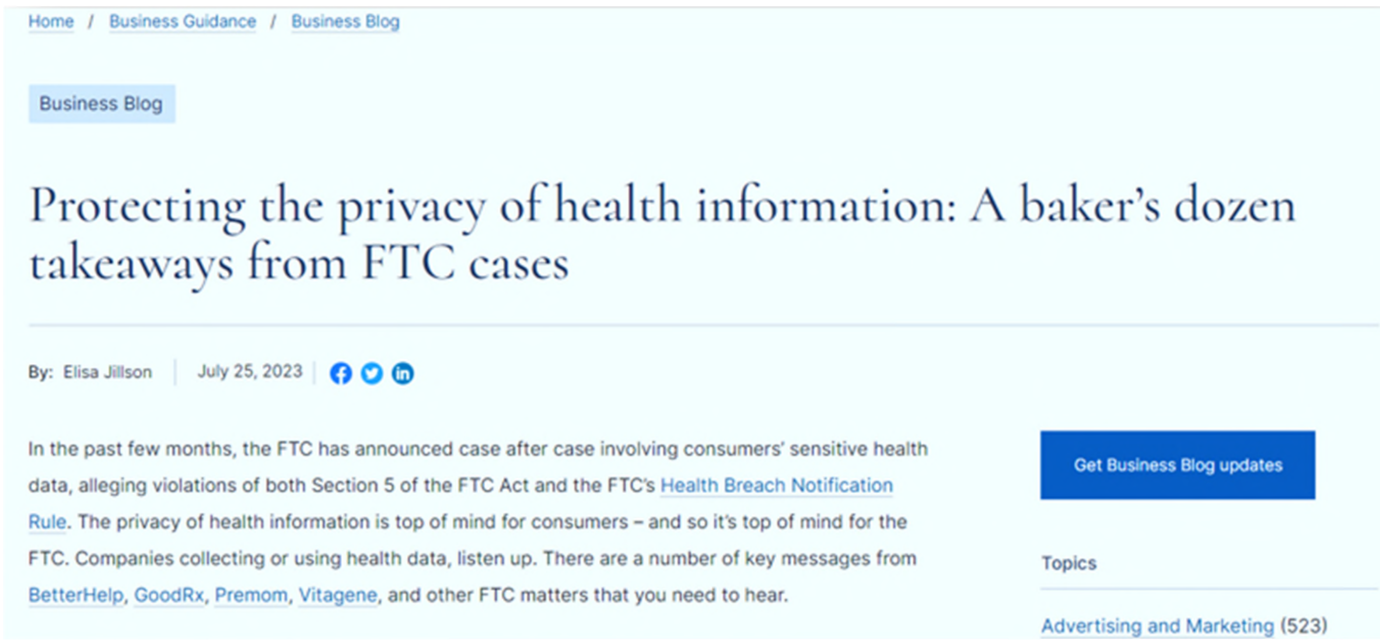
Re: Use of Online Tracking Technologies

Dear [Name of Recipient],

The Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) and the Federal Trade Commission (FTC) are writing to draw your attention to serious privacy and security risks related to the use of online tracking technologies that may be present on your website or mobile application (app) and impermissibly disclosing consumers' sensitive personal health information to third parties.

Recent research,[1] news reports,[2] FTC enforcement actions,[3] and an OCR bulletin[4] have highlighted risks and concerns about the use of technologies, such as the Meta/Facebook pixel and Google Analytics, that can track a user's online activities. These tracking technologies

FTC Publishes Blog on Website Health Info Privacy



Home / Business Guidance / Business Blog

Business Blog

Protecting the privacy of health information: A baker's dozen takeaways from FTC cases

By: Elisa Jillson | July 25, 2023

In the past few months, the FTC has announced case after case involving consumers' sensitive health data, alleging violations of both Section 5 of the FTC Act and the FTC's Health Breach Notification Rule. The privacy of health information is top of mind for consumers – and so it's top of mind for the FTC. Companies collecting or using health data, listen up. There are a number of key messages from BetterHelp, GoodRx, Premom, Vitagene, and other FTC matters that you need to hear.

Get Business Blog updates

Topics

Advertising and Marketing (523)

AHA sues HHS Over Online Tracking Guidance (November 2023)

- AHA joined by Texas Hospital Association, Texas Health Resources, and United Regional Heath Care System
- Seeks declaratory judgment
- Alleges bulletin exceeds statutory authority
- Alleges HHS's website is inconsistent with bulletin

American Hospital Association

Hospital associations and hospitals file lawsuit challenging federal rule that ties providers' hands in efforts to reach communities

Nov 02, 2023 - 04:01 PM

The AHA, joined by the Texas Hospital Association, Texas Health Resources, and United Regional Health Care System, Nov. 2 sued (https://www.aha.org/legal-documents/2023-11-02-case-complaint-aha-tha-thr-united-health-care-system-v-rainer) the federal government to bar enforcement of an unlawful, harmful and counterproductive rule that has upended hospitals' and health systems' ability to share health care information with the communities they serve, analyze their own websites to enhance accessibility, and improve public health.

OCR Updates Guidance on Online Tracking (Mar. 18, 2024)

- Focuses on intent of website visitor.
  - Student visiting hospital’s oncology webpage to write term paper is not PHI about student.
  - Individual visiting same page to seek a second opinion on treatment options for a brain tumor is PHI.
- Indicates an enforcement priority on whether Security Rule risk analysis addresses website disclosure risks.

AHA wins lawsuit (June 20, 2024)

- “Simply put, Identity (Person A) + Query (Condition B) ≠ IIHI (Person A has Condition B).”
- Declared the guidance unlawful and vacated with respect to the “Proscribed Combination” of “circumstances where an online technology connects (1) an individual's IP address with (2) a visit to a [unauthenticated public webpage] addressing specific health conditions or healthcare providers.”
- Does <u>not</u> seek to declare the remainder of the guidance unlawful.
- OCR updated its bulletin, indicating that “HHS is evaluating its next steps in light of [the] order.”

Largest threat remains class action lawsuits:

LOCAL NEWS

NC hospital system settles patients Meta Pixel lawsuit for $6.6 million

Mass General Brigham Settles 'Cookies Without Consent' Lawsuit for $18.4 Million

Advocate Aurora settles pixel suit for $12M

Naomi Diaz - Thursday, August 17th, 2023

Confidentiality of Substance Use Disorder Patient Treatment Records

42 C.F.R. Part 2

- Applies to:
  - Federally-assisted "programs":
    - Specialty facilities or individuals who hold themselves out as providing, and provides, substance use disorder diagnosis, treatment, or referral for treatment ("SUD services");
    - Identified unit within general medical facility that holds itself out as providing, and provides, SUD services; or
    - Medical personnel or other staff within general medical facility whose primary function is provision of SUD services and is identified as such a provider.
  - Qualified service organizations (service providers)
  - Lawful holders (receive SUD records pursuant to a consent)
- More stringent than HIPAA with respect to limits on uses and disclosures of SUD records

February 2024 Final 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 provide one-time authorization for all uses and disclosures of Part 2 Records for treatment, payment, and health care operations (“TPO”)
- HIPAA-regulated recipient of Part 2 Records generally can further use and disclose as permitted under HIPAA [Limited to records received pursuant to TPO consent?]

February 2024 Final Rule (continued)

- 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

February 2024 Final Rule (continued)

- Likely impact:
  - Continued need to segregate data
  - Increased risk of enforcement
- Remaining question: If patient provides limited consent, can CE/BA recipient use and disclose to the extent permitted by HIPAA?
- Compliance date: February 16, 2026

State Consumer Health Data Privacy Laws

States with General Privacy Laws

State	Threshold*	PHI Exempt	CE/BA Exempt	Nonprofits Exempt	Date
California	$25M or 100,000 CA residents	Yes (in hands of CE/BA)	No	Generally yes	Jan. 1, 2020
Colorado	100,000 CO residents	Yes (in hands of CE/BA)	No	No	July 1, 2023
Connecticut	100,000 CT residents	Yes	Yes	Yes	July 1, 2023
Delaware	35,000 DE residents	Yes	No	No	Jan. 1, 2025
Florida	$1B and smart speaker or app store	Yes	Yes	Yes	July 1, 2024
Indiana	100,000 IN residents	Yes	Yes	Yes	Jan. 1, 2026
Iowa	100,000 IA residents	Yes	Yes	Yes	Jan. 1, 2025

States with General Privacy Laws

State	Threshold*	PHI Exempt	CE/BA Exempt	Nonprofits Exempt	Date
Kentucky	100,000 KY residents	Yes	Yes	Yes	Jan. 1, 2026
Maryland	35,000 MD residents	Yes	No	No	Oct. 1, 2025
Minnesota	100,000 MN residents	Yes	No	No	July 31, 2025
Montana	50,000 MT residents	Yes	Yes	Yes	Oct. 1, 2024
Nebraska	Processes or engages in sale of personal data	Yes	Yes	Yes	Jan. 1, 2025
New Hampshire	35,000 NH residents	Yes	Yes	Yes	Jan. 1, 2025
New Jersey	100,000 NJ residents	Yes	No	Yes	Jan. 15, 2025

States with General Privacy Laws

State	Threshold*	PHI Exempt	CE/BA Exempt	Nonprofits Exempt	Date
Oregon	100,000 OR residents	Yes (processed by CE/BA)	No	No	July 1, 2024
Rhode Island	35,000 RI residents	Yes	Yes	Yes	Jan. 1, 2026
Tennessee	$25M and 175,000 TN residents	Yes	Yes	Yes	July 1, 2025
Texas	Process or engage in sale of personal data	Yes	Yes	Yes	July 1, 2024
Utah	$25M and 100,000 UT residents	Yes	Yes	Yes	Dec. 31, 2023
Virginia	100,000 VA residents	Yes	Yes	Yes	Jan. 1, 2023

State Consumer Health Privacy Laws

- Passed in Washington, Nevada, and Connecticut, with New York awaiting Governor’s signature.
- Consent requirements for collection of consumer health data (CHD) other than to deliver requested product or service.
- Strong notice requirements (WA AG requires separate CHD notice)
- Strong transparency requirements (e.g., listing of third-party recipients)
- Strong privacy rights (such as right of deletion without exception)

FTC Enforcement of Health Privacy

Recent Enforcement Actions

GoodRx (2/1/23)

- Disclosure of website data to third parties advertising platforms
- Section 5 + HBNR
- $1.5 million civil monetary penalty

BetterHelp (3/2/23)

- Disclosure of website data to third parties advertising platforms
- Section 5
- $7.8 payment to consumers

Premom (5/17/23)

- Disclosure of website data to third parties advertising platforms
- Section 5 + HBNR
- $100,000 civil monetary penalty

1Health.io (6/16/23)

- Failure to destroy samples, failure to get opt in to change in privacy policy, lack of security
- Section 5
- $75,000 payment for consumer refunds

Recent Enforcement Actions

Monument (4/11/24)

- Disclosure of website data to third parties advertising platforms
- Section 5 + Opioid Addiction Recovery Fraud Prevention Act
- $2.5M civil monetary penalty

Cerebral (4/15/24)

- Disclosure of website data to third parties advertising platforms
- Section 5 + Opioid Addiction Recovery Fraud Prevention Act
- $15M civil monetary penalty ($8M suspended)

Health Breach Notification Rule (HBNR)

- Conforms regulations to September 2021 Policy Statement
- Applies HBNR to broad range of health and wellness apps
- Clarifies that “breach of security” includes any use or disclosure not authorized by consumer
- Provides more time to notify FTC

Billing Code: 6750-01P

FEDERAL TRADE COMMISSION

16 CFR Part 318

RIN 3084-AB56

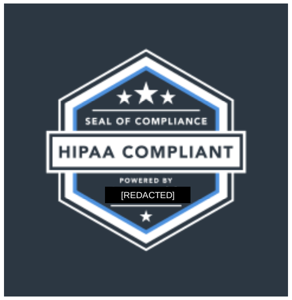
Health Breach Notification Rule

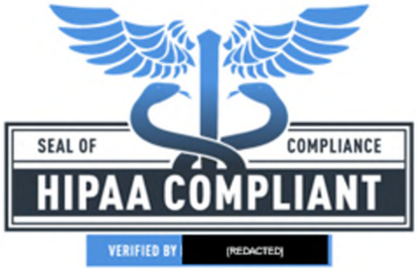
AGENCY: Federal Trade Commission.

ACTION: Final rule.

SUMMARY: The Federal Trade Commission (“FTC” or “Commission”) is amending the Commission’s Health Breach Notification Rule (the “HBN Rule” or the “Rule”). The HBN Rule requires vendors of personal health records (“PHRs”) and related entities that are not covered by the Health Insurance Portability and Accountability Act (“HIPAA”) to notify individuals, the FTC, and, in some cases, the media of a breach of unsecured personally identifiable health data. The amendments: (1) clarify the Rule’s scope, including its coverage of developers of many health applications (“apps”); (2) clarify what it means for a vendor of personal health records to draw PHR identifiable health information from multiple sources; (3) revise the definition of

Hunting for HIPAA Targets …





Potential Future

- Section 5 Enforcement
  - Likely to lesson; and
  - More straightforward cases, less envelope-pushing.

- HBNR
  - Continue to enforce;
  - Silently stop enforcing; or
  - Revert to more narrow statutory interpretation through notice-and-comment rulemaking.

Adam Greene

Partner, Washington, DC
David Wright Tremaine

adamgreene@dwt.com
P: 202.973.4213