Update on HIPAA and Other Health Information Privacy and Security Developments

Spring 2026 Privacy+Security Forum

Adam Greene

Partner
Davis Wright Tremaine LLP

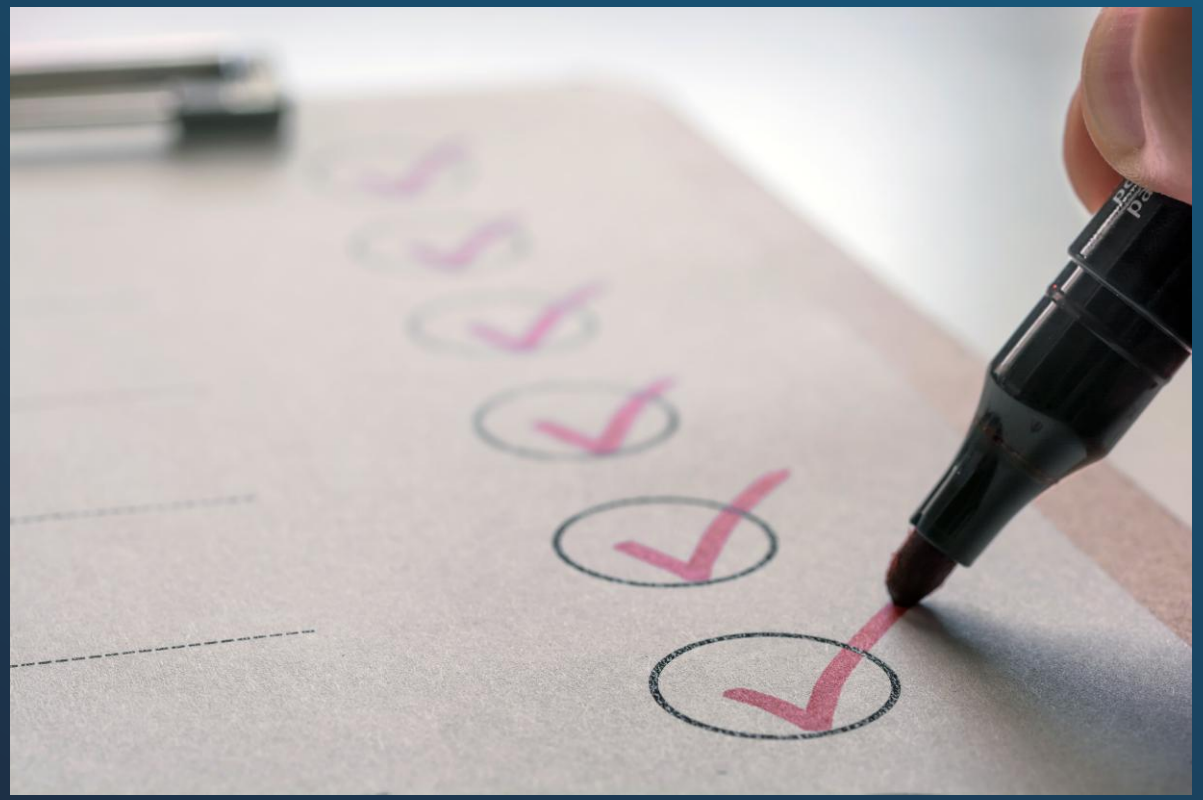
Timothy Noonan

Deputy Director for Health Information Privacy, Data, and Cybersecurity
HHS Office for Civil Rights

Wednesday, May 6, 2026

Agenda

- OCR Update on Rulemakings and Enforcement
  - Confidentiality of Substance Use Disorder Patient Records
  - HIPAA Privacy Rule NPRM
  - HIPAA Security Rule NPRM
  - Recent Enforcement Actions
  - Enforcement Initiatives
  - HIPAA Audits
  - HIPAA Videos
- And the rest …
  - FTC Enforcement of Health Privacy
  - DOJ Bulk Sensitive Data Rule
  - State Health Privacy Law Trends
  - De-Identified Health Data
  - Health Privacy Litigation Trends
  - Health Privacy Hot Topics



Confidentiality of Substance Use Disorder Patient Records under 42 CFR part 2 ("Part 2") Final Rule

- Modifies Part 2 to increase coordination among providers treating patients for substance use disorders, strengthens confidentiality protections through civil enforcement, and enhances integration of behavioral health information with other medical records to improve patient health outcomes. The final rule includes the following changes
  - Permits use and disclosure of Part 2 records based on a single patient consent, given once, for all future uses and disclosures for treatment, payment, and health care operations.
  - Permits redisclosure of Part 2 records by HIPAA covered entities and business associates in accordance with the HIPAA Privacy Rule, with certain exceptions.
  - Establishes patient rights with respect to Part 2 records.
  - Aligns Part 2 Patient Notice requirements with the HIPAA Notice of Privacy Practices requirements.
  - Requires breach notification for breaches of Part 2 records.
  - Provides HHS with civil enforcement authority, including the potential imposition of civil money penalties for violations of Part 2.
- Final Rule at https://www.federalregister.gov/public-inspection/2024-02544/confidentiality-of-substance-use-disorder-patient-records.
- Fact sheet at https://www.hhs.gov/hipaa/for-professionals/regulatory-initiatives/fact-sheet-42-cfr-part-2-final-rule/index.html.
- Compliance Date: February 16, 2026

Proposed Modifications to the HIPAA Privacy Rule to Support, Remove Barriers to Coordinated Care, and Individual Engagement

- Published in the Federal Register on January 21, 2021.
- Sought public comment on proposals to modify the HIPAA Privacy Rule to improve health information sharing for more effective heath care, empower individuals with their own health information, and lift unnecessary administrative burdens on covered health care providers and health plans.

Confidentiality of Substance Use Disorder Patient Records

- NPRM Fact Sheet: https://www.hhs.gov/sites/default/files/hipaa-nprm-factsheet.pdf
- The public comment period closed on May 6, 2021. Over 1,400 comments received.
- Comments available at https://www.regulations.gov/document/HHS-OCR-2021-0006-0001
- Spring 2025 Unified Agenda: https://www.reginfo.gov/public/do/eAgendaMain

Proposed Modifications to HIPAA Security Rule to Strengthen Cybersecurity for ePHI

- Published in the Federal Register on January 6, 2025.
- Proposes to strengthen the requirements for HIPAA regulated entities to safeguard electronic protected health information to prevent, detect, contain, mitigate, and recover from cybersecurity threats.
- NPRM available at: https://www.govinfo.gov/content/pkg/FR-2025-01-06/pdf/2024-30983.pdf
- NPRM Fact Sheet: https://www.hhs.gov/hipaa/for-professionals/security/hipaa-security-rule-nprm/factsheet/index.html
- The public comment period closed on March 7, 2025. More than 4,700 comments received.
- Comments available at https://www.regulations.gov/document/HHS-OCR-2024-0020-0001.

Recently Announced OCR HIPAA Enforcement Actions

May-25	Vision Upright MRI	$5,000
May-25	BayCare Health System	$800,000
May-25	Comstar, LLC	$75,000
Jun-25	Deer Oaks – The Behavioral Health Solution	$225,000
July-25	Syracuse ASC	$250,000
Aug-25	BST & Co CPAs, LLP	$175,000
Sep-25	Cadia Healthcare Facilities	$182,000
Dec-25	Concentra, Inc	$112,500
Feb-26	Top of the World Ranch Treatment Center	$103,000
Mar-26	MMG Fusion, LLC	$10,000
Apr-26	Regional Women's Health Group, LLC	$320,000
Apr-26	Assured Imaging Affiliated Covered Entities	$375,000
Apr-26	Consociate, Inc.	$225,000
Apr-26	Star Group. L.P. Health Benefits Plan	$245,000

Right of Access Initiative

- HIPAA Privacy Rule gives individuals a right to timely access to their health records (30 days with a possibility of one 30-day extension), and at a reasonable, cost-based fee.
- OCR receives many complaints alleging denial or no access to health records.
- 54 completed enforcement actions.
- More information on HIPAA right of access available at: https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html

Risk Analysis Initiative

- Focus on compliance with key HIPAA Security Rule requirement.
- Most OCR large breach investigations reveal a lack of a compliant risk analysis.
- 13 completed enforcement actions in this initiative.
- Recently expanded to include risk management requirement.

HIPAA Audits

- Audits initiated in December 2024.
- Reviewing compliance with selected provisions of the HIPAA Security Rule most relevant to hacking and ransomware attacks.
- OCR will publish an industry report summarizing OCR's findings after the Audits are completed.
- HIPAA Audits webpage: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html

HIPAA Videos

- *New* **Risk** Management Video https://www.youtube.com/watch?v=kDyrj-fJzhw
- Ransomware and the HIPAA Security Rule Video https://www.youtube.com/watch?v=nBKUlAy1OFA
- Common Cyber-Attacks Video http://youtube.com/watch?v=VnbBxxyZLc8
- HIPAA Risk Analysis Webinar https://www.youtube.com/watch?v=hxfxhokzKEU
- Recognized Security Practices Video https://www.youtube.com/watch?v=e2wG7jUiRjE

Relevant Health Privacy Laws

- Federal
  - HIPAA
  - 42 C.F.R. Part 2
  - Section 5 of the FTC Act
  - FTC Health Breach Notification Rule (HBNR)
  - DOJ Bulk Sensitive Personal Data Rule
- State
  - Medical privacy laws
  - Sensitive condition laws
  - General consumer privacy laws
  - Consumer health data laws
  - Breach notification laws
  - Unfair, Deceptive, and Abusive Practices laws
- International

My OCR Predictions

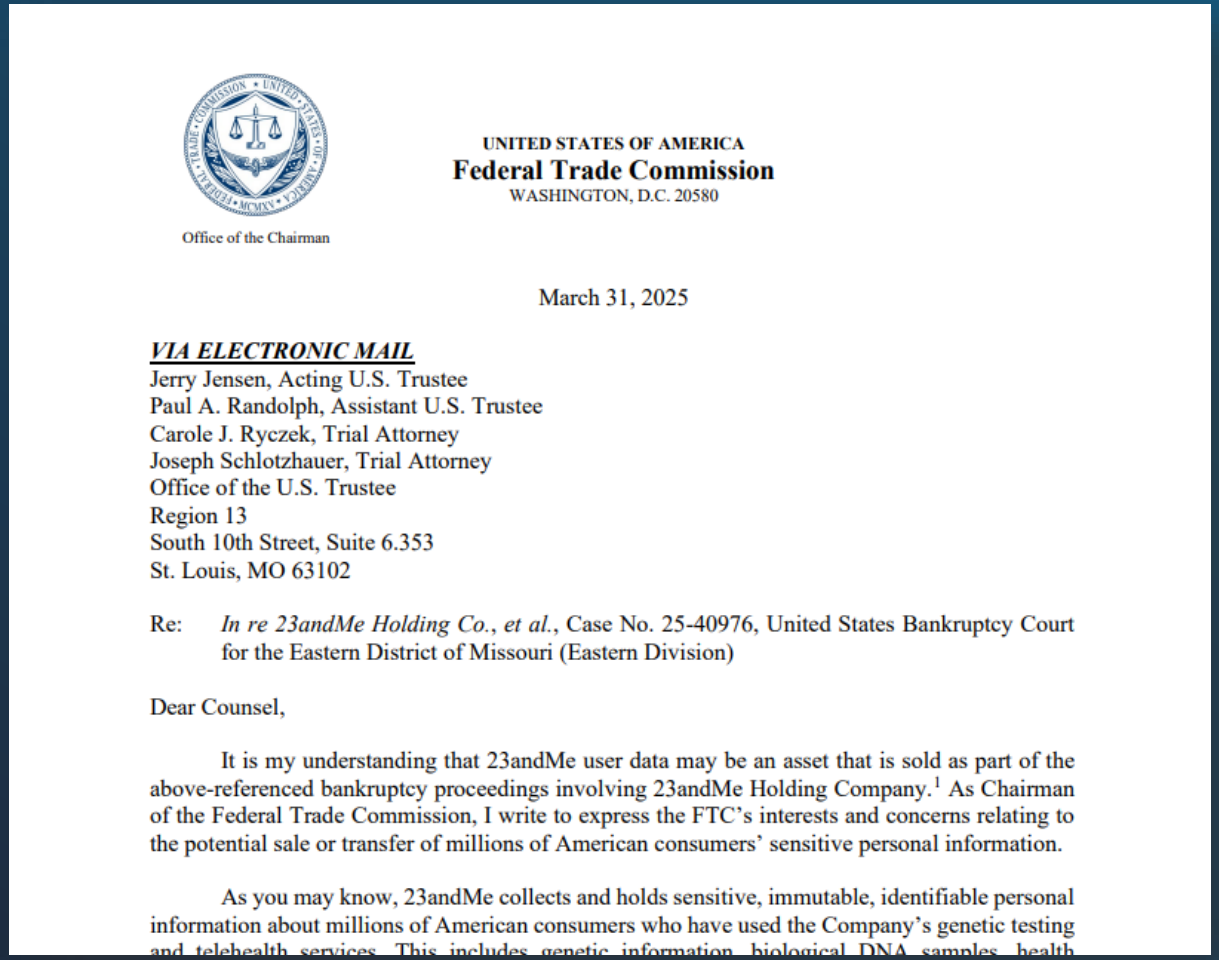
- Enforcement posture unlikely to change
- Resolution of cases likely will take longer
- Privacy Rule NPRM likely to be finalized similar to proposal
- Security Rule NPRM likely to look very different from proposal
- Increased risk of 42 C.F.R. part 2 enforcement

Federal Trade Commission (FTC)

- Section 5 of the FTC Act
  - Prohibits unfair and deceptive trade practices
  - Generally, does not apply to nonprofits
- Health Breach Notification Rule
  - Applies to:
    - Personal health record (PHR) vendors
    - PHR related entities
    - Third party service providers
  - FTC interpreted that any unauthorized use or disclosure of PHR identifiable health information is a “breach.”
  - FTC has broadly interpreted scope of “PHR” to encompass range of consumer health apps.

FTC Trends

- FTC commission provided letter to trustee regarding ensuring privacy of genetic information in 23andMe bankruptcy.
- No indication of continued focus on website disclosures.
- No indication of continued broad interpretation of Health Breach Notification Rule.



Office of the Chairman

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

March 31, 2025

VIA ELECTRONIC MAIL
Jerry Jensen, Acting U.S. Trustee
Paul A. Randolph, Assistant U.S. Trustee
Carole J. Ryczek, Trial Attorney
Joseph Schlotzhauer, Trial Attorney
Office of the U.S. Trustee
Region 13
South 10th Street, Suite 6.353
St. Louis, MO 63102

Re: *In re 23andMe Holding Co., et al.*, Case No. 25-40976, United States Bankruptcy Court for the Eastern District of Missouri (Eastern Division)

Dear Counsel,

It is my understanding that 23andMe user data may be an asset that is sold as part of the above-referenced bankruptcy proceedings involving 23andMe Holding Company.[1] As Chairman of the Federal Trade Commission, I write to express the FTC's interests and concerns relating to the potential sale or transfer of millions of American consumers' sensitive personal information.

As you may know, 23andMe collects and holds sensitive, immutable, identifiable personal information about millions of American consumers who have used the Company's genetic testing and telehealth services. This includes genetic information, biological DNA samples, health

DOJ Bulk Sensitive Personal Data Rule

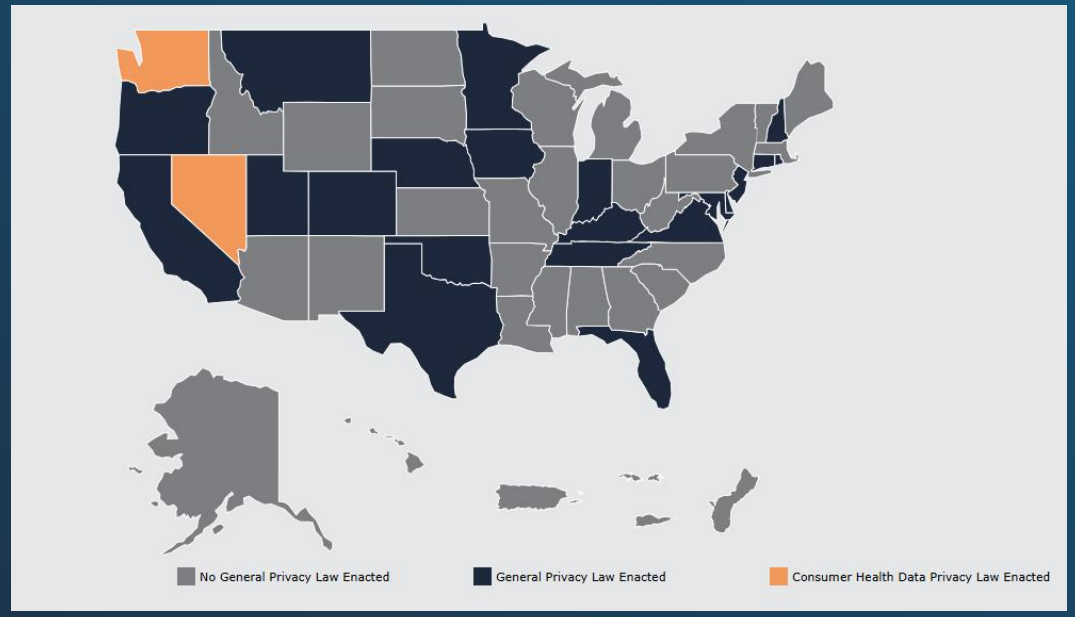
- New kid on the block – January 8, 2025
- Applies to data brokering of health data of over 10,000 U.S. persons, even if de-identified.
- Prohibits sale or license to countries of concern (China, Cuba, Iran, North Korea, Russia, and Venezuela) and related “covered persons.”
- Requires contractual restrictions for covered transaction with any foreign person.

State Medical Privacy Laws

- Govern all or some kinds of health care providers.
- Sometimes govern other types of entities (California and Texas are particularly broad).
- Typically govern disclosures, but some may govern internal uses of data too.
- Scope varies (e.g., PHI, “medical information,” “medical records,” etc.).
- Relatively stable other than addition of reproductive health and gender affirming care and immigration enforcement.

State Consumer Privacy Laws

- Started with California Consumer Privacy Act in 2018.
- As of March 23, 2026, 21 states have enacted general consumer privacy laws governing personal information.
- Govern identifiable personal information, with additional limits on sensitive personal information (such as health information).



State Consumer Privacy Law Requirements

Data Inventory & Mapping

- Know what personal data you collect, use & share
- Conduct data flow mapping across all systems
- Document data categories and processing purposes

Consumer Rights

- Rights to access, deletion, correction & portability
- Respond within 45–90 days; verify requestor identity
- Non-discrimination required for rights exercised

Opt-Out Mechanisms

- Honor "Do Not Sell/Share" requests
- Opt-out of targeted advertising & profiling
- Honor Global Privacy Control (GPC) signals where required

Vendor Contracts

- Data processing agreements with all service providers
- Limit use to the specified purpose only
- Flow-down obligations to subprocessors

Privacy Notices

- Disclose categories collected, purpose & third-party sharing
- Provide notice at or before point of collection
- Keep privacy policy accessible and current

Data Security

- Implement reasonable technical & organizational safeguards
- Apply data minimization and purpose limitation
- Enforce retention limits and timely deletion

State Consumer Privacy Law Analysis

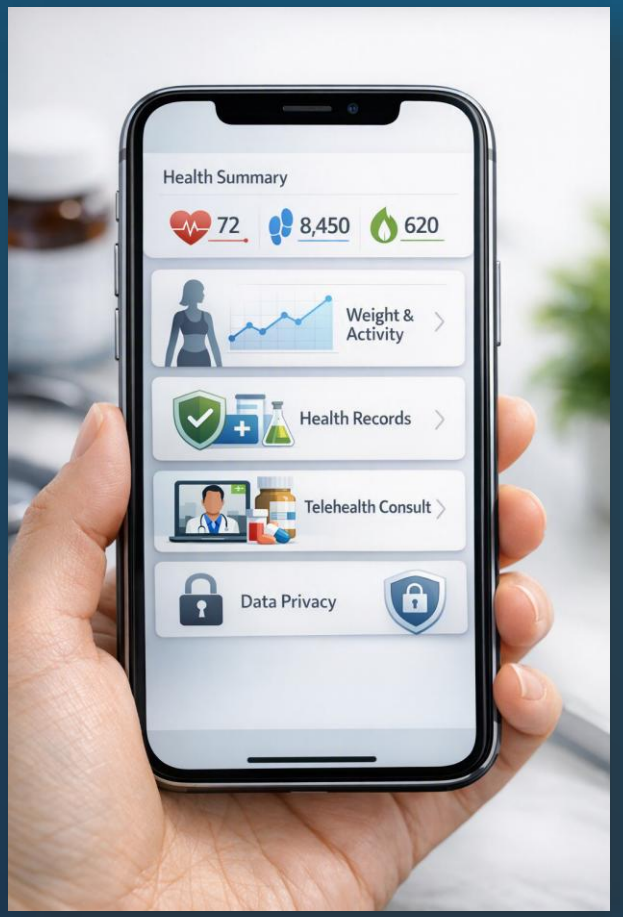
State	HIPAA Exemption19	Nonprofit Exemption	Applicability Threshold
California	PHI	Generally	$26,625,000 revenue or 100,000 residents
Colorado	PHI	No	100,000 residents
Connecticut	CE/BA/PHI	Yes	35,000 residents or processing of any sensitive personal data
Delaware	PHI	No	35,000 residents
Indiana	CE/BA/PHI	Yes	100,000 residents
Iowa	CE/BA/PHI	Yes	100,000 residents
Kentucky	CE/BA/PHI	Yes	100,000 residents
Maryland	PHI	No	35,000 residents
Minnesota	PHI	No	100,000 residents
Montana	CE/BA/PHI	Yes	25,000 residents
Nebraska	CE/BA/PHI	Yes	No minimum
New Hampshire	CE/BA/PHI	Yes	35,000 residents
New Jersey	PHI	No	100,000 residents
Oklahoma	CE/BA/PHI	Yes	100,000 residents
Oregon	PHI	No	100,000 residents
Rhode Island	CE/BA/PHI	Yes	35,000 residents
Tennessee	CE/BA/PHI	Yes	$25,000,000 revenue and 175,000 residents
Texas	CE/BA/PHI	Yes	No minimum
Utah	CE/BA/PHI	Yes	$25,000,000 revenue and 100,000 residents
Virginia	CE/BA/PHI	Yes	100,000 residents

State Consumer Privacy Law Analysis

- Step 1 – If subject to HIPAA, does a HIPAA entity-level exemption apply?
- Step 2 – If you are a nonprofit, does the state law include a nonprofit exemption?
- Step 3 – Do you meet the state law's applicability threshold?

State Consumer Health Data Laws

- Washington enacted the My Health My Data Act in 2023.
- Focused on filling the gaps left by HIPAA.
- Nevada passed a similar law. Connecticut incorporated similar provisions into its general consumer privacy law.
- New York almost passed a consumer health privacy law in 2025.
- Like general consumer privacy laws, but more stringent.



State Health Privacy Law Trends

- State medical privacy laws are stable, other than potential additions regarding reproductive health and gender affirming care and immigration enforcement.
- State consumer privacy laws are becoming more stringent with respect to sensitive personal information, and California brought enforcement action under CCPA related to health data.
- No significant enforcement of state consumer health data laws yet, but NY almost passed the most stringent consumer health data law in US.

De-Identified Health Data

- DOJ Bulk Sensitive Data Rule
  - May not sell or license 10,000 or more records to country of concern or related covered person.
  - Must pass on contractual restrictions to any foreign person.
- CCPA contractual provisions:
  - A statement that the de-identified information being sold or licensed includes de-identified patient information.
  - A statement that re-identification, and attempted re-identification, of the de-identified information by the purchaser or licensee of the information is prohibited pursuant to Cal. Civ. Code § 1798.148.
  - A requirement that, unless otherwise required by law, the purchaser or licensee of the de-identified information may not further disclose the de-identified information to any third party unless the third party is contractually bound by the same or stricter restrictions and conditions.

De-Identified Health Data

- Administrative de-identification requirements (if state law does not exempt HIPAA de-identified data)
  - Take reasonable measures to ensure that such data cannot be associated with an individual.
  - Publicly commit to process such data only in a de-identified fashion and not attempt to re-identify such data.
  - Contractually obligate any recipients of such data to comply with above.

Health Privacy Litigation Trends

- Wiretapping cases over website disclosures.
- First class action over ambient AI (under wiretapping theory).
- Continued data breach litigation.

Health Privacy Hot Topics

- AI, AI, AI
- Ambient AI
- Website disclosure litigation
- HIE breaches
- Immigration enforcement
- Reproductive health and gender affirming care

Questions?

Adam Greene

Partner, Washington, DC
David Wright Tremaine

adamgreene@dwt.com
P: 202.973.4213

Timothy Noonan

Deputy Director for Health Information Privacy, Data, and Cybersecurity
HHS Office for Civil Rights