POLSINELLI

HIPAA/Health Information Privacy & Security

The explosion of digital data, along with the proliferation of technology, devices and other health care innovations has created a multilayered range of privacy and data security issues in the health care industry. Polsinelli's multidisciplinary Health Information Privacy & Security group brings together attorneys across the firm focusing on the areas of privacy, security, technology and litigation, who understand the value of your health-related data and are adept at assisting clients in maximizing the benefits of that data while minimizing and responding to ever-changing threats and risks.

Our team has deep experience in the full breadth of privacy/security-related laws and regulations impacting the health care industry, including HIPAA, FERPA, federal laws and regulations governing the confidentiality of alcohol and drug use treatment records, state privacy/security laws related to the confidentiality of health information (including mental health, HIV/AIDS and genetic information), and international privacy laws impacting data use and transfers including without limitation, the EU General Data Protection Regulation (GDPR) and similar laws in other countries outside the U.S.

Attorneys in the practice have the skills to advise you on complex data-sharing arrangements, data protection strategies, and security incident or data breach response plans. Our team includes:

- A former Acting Deputy Director and Senior Advisor for HIPAA Compliance and Enforcement for the Office for Civil Rights (OCR) who was responsible for the growth of the HIPAA Enforcement program from 2012 to 2017 and who is a Certified Information Systems Security Professional (CISSP)
- A former Office for Civil Rights (OCR) attorney who assisted in conducting OCR Phase I audits, drafting the 2013 Final Rule and performing OCR breach investigations with a particular focus on breaches affecting 500 or more individuals
- A former OCR attorney who assisted in drafting and negotiating settlement agreements and served as the lead investigator of several high-profile investigations, including one of OCR's largest settlements to date
- Attorneys who have obtained the Certified Information Privacy Professional-U.S. designation (CIPP/US) and the CIPP-Europe (CIPP/E) from the International Association of Privacy Professionals
- Litigators who have appeared in state and federal courts around the country related to health care data privacy and security issues
- Former in-house counsel who understand business realities and the need to provide practical guidance accurately, quickly and efficiently
- Technology lawyers who understand your electronic systems and can work with your IT team to address security issues, including cyber-attack avoidance and response

Our recent rankings include national recognition from *Chambers USA: America's Leading Lawyers for Business* in Privacy & Data Security: Healthcare, 2023. We offer a diversity of comprehensive services to health care clients, including:

- Advising on structuring complex data sharing arrangements to overcome restrictions on sharing for purposes of clinically integrated networks, via health information exchanges and for marketing, among other purposes
- Structuring privacy and security compliance programs and facilitating risk management
- Assisting with incident response and breach reporting, including counseling on OCR compliance reviews, HIPAA audits or other government investigations
- Advising on mobile devices, wearables and other digital products, including advising on privacy by design in the product development stage, conducting data protection impact assessments and reviewing website applications and devices for HIPAA and international privacy law compliance
- Assisting in litigation matters, including civil lawsuits and class actions alleging violations of privacy or security under various federal and/or state laws and representation in TCPA actions
- Advising on transactions/due diligence, including drafting appropriate representations and warranties on privacy and security-related matters and reviewing HIPAA and other privacy-related policies and procedures, security risk analyses and risk management plans, business associate agreements, data processing agreements, breach logs, and other key documentation to evaluate compliance and assess risk
- Assisting with HIPAA compliance for clients' group health plans and advising on the unique privacy and security issues beyond HIPAA implicated by wellness programs and employer-sponsored clinics, including state privacy laws and occupational health laws and regulations

Matters

Government Investigations/Enforcement Actions

- Following a four-year OCR investigation negotiated a resolution agreement and corrective action plan with OCR on behalf of a large health system arising out of a breach involving thousands of patients. A substantial reduction to the settlement amount that OCR initially proposed was negotiated, and favorable corrective action plan terms for the client were established.
- Assisted a physician practice in investigating a complicated ransomware attack, including hiring a forensic analyst on a privileged basis to determine the scope of an attack and whether there was evidence of exfiltration or malware left on the system. We also analyzed whether the attack rose to the level of a reportable breach, taking into account OCR's recent guidance on ransomware attacks.
- Assisted a university/academic medical center client in responding to and successfully obtaining a determination from OCR to close, without imposition of penalties, its investigation of the client arising out of a lost laptop containing the PHI of thousands of patients. In addition, we successfully challenged the scope of an OCR document request.
- Assisted a large hospital in successfully responding to a phishing attack that impacted over a thousand patients. As part of representation, a security consultant was engaged on a privileged basis to pinpoint the attack's scope and identify the appropriate mitigation and corrective action steps. Assisted the client in responding to the subsequent OCR investigation, which included responding to initial and follow-up questions and document requests and ultimately resulted in OCR closing the investigation without imposing any penalties against the client.
- Represented a physician practice in connection with the theft of a desktop computer containing PHI of thousands of patients. Assisted the client through the investigation, breach reporting process, remediation/mitigation efforts and successfully obtained a determination from OCR to close, without penalties, its investigation based on jurisdictional grounds.
- Assisted a large hospital client in obtaining closure, without penalties, of an OCR investigation stemming from a breach that occurred at the business associate level involving electronic PHI of thousands of patients. Counseled the client through all aspects of the breach, including assisting the client in its investigation of the breach and the business associate's actions, making the required notifications and preparing its response to the OCR investigation and document request, which ultimately resulted in OCR closing the investigation as to the client.

- Successfully convinced the California Department of Public Health to withdraw a penalty notice and close out an investigation into a national provider client in connection with a theft of patient information from an employee's car.

OCR HIPAA Audit Preparation

- Assisted a national hospice client who received notification from OCR of a pending HIPAA audit in preparing for the audit, including reviewing the client's privacy and security policies, procedures and processes for compliance gaps and providing recommendations for improvement.
- Analyzed the HIPAA practices of a provider with locations in all 50 states against the OCR audit protocol.
- Analyzed a large hospital's HIPAA policies and procedures and revised the policies to incorporate issues highlighted in the OCR audit protocol.

Global Privacy Program Development & Implementation

- Assisted multinational health care companies with development and implementation of their global privacy programs, including data mapping to meet requirements under privacy laws, including GDPR and CCPA, policy and procedure preparation and implementation, and development of template privacy notices, consents, and data processing agreements, among others.
- Supported product teams in compliance with international privacy requirements as necessary to support successful product launches.

HIEs, CINs & Structuring Complex Data Sharing Arrangements

- Guided a statewide health information exchange (HIE) through its formation, governance and consent model. Assisted the client by developing participation agreements and policies, and procedures and advising on ongoing operational issues. Work included analyzing various state law issues that impacted the consent model, as well as interfacing with various health care provider participants and the state Medicaid program.
- Advised a large health care system that operates in several states on the creation and implementation of a private HIE. Created agreements, policies and procedures and worked with internal business departments on desired data use scenarios.
- Assisted a client offering HIE and data analytics services in multiple states, including advising on state information privacy and health information exchange laws, HIPAA and 42 CFR Part 2 preemption issues, and consent models in multiple states, and preparing corresponding participation agreements and operating policies and procedures.

Security & Technology, Health Information Systems

- Assisted a client through the privacy and security compliance considerations and operational issues in operating and offering a shared electronic health record platform to unaffiliated community providers.
- Assisted a large health system in implementing its patient portal, including drafting terms of use, privacy policy, etc.
- Regularly worked with security consultants (or hired security consultants on a privileged basis) on behalf of health care clients to perform security assessments, including enterprise-wide risk analyses, penetration testing, forensic analysis, etc.

Marketing Initiatives, Including Online Activities

- Worked closely with a number of provider clients on privacy/security aspects of website retargeting campaigns, including reviewing and revising website privacy policies to make sure the language is "clear and conspicuous" under the FTC standards and in compliance with state laws.
- Advised a large hospital client on various privacy and security laws (including HIPAA, the FTC's Telemarketing Sales Rule and the FCC's TCPA) in providing appointment reminders through automated/prerecorded voice and text communications.

- Regularly advised provider clients on privacy and security issues relating to marketing initiatives, including restrictions under HIPAA, the TCPA, CAN-SPAM and various state laws, such as California's Confidentiality of Medical Information Act (CMIA).

Big Data Use & Analytics, Assisting with De-Identification

- Advised an international provider on their big data analytics strategy, including addressing HIPAA and international data transfer issues as well as data governance rules.
- Worked closely with statisticians to prepare determinations of de-identification for provider clients so the clients could report data to manufacturers and other third parties.
- Regularly reviewed contracts and data reporting provisions for health care clients to determine if the proposed reporting meets the de-identification requirements.

Clinical Research Issues

- Assisted a large hospital in creating a data warehouse and tissue bank for research. Representation included advising on HIPAA and state privacy and security requirements, structuring appropriate use cases, and addressing data ownership issues.
- Advised a large academic medical center acting as a coordinating center in an international clinical trial on compliance with US and international privacy and security requirements.
- Advised a national nonprofit organization on the state privacy law requirements impacting its informed consent/authorization form and secondary uses of data.
- Assisted research study sponsors in addressing data privacy issues with multi-center international clinical trials.

Transactions, Due Diligence on Privacy, Security Issues

- After discovering through due diligence that a target provider had been the subject of a ransomware attack affecting its electronic systems, counseled the potential buyer (a large health system) on the scope of the attack and how to evaluate and address the risks in moving forward with the transaction.
- Assisted a national provider in evaluating and quantifying risk in moving forward with an acquisition of a multi-location physician practice that lacked a HIPAA privacy/security program. Work included drafting contractual protections and identifying pre- and post-closing steps to address significant risks.
- Reviewed over 50 business associate agreements on behalf of a client purchasing a business associate to evaluate HIPAA compliance and the assignment provisions and to determine whether off-shoring of PHI was prohibited.

Publications

2026
When cyberattacks disrupt care processes, pay attention to these 3 Cs
Featured, HIMSS TV Podcast

April 21, 2026
5 ways your doctor may be using AI chatbots — and why it matters
Quoted, CNN

December 8, 2025
Critical Deadline to Update Notices of Privacy Practices Related to Substance Use Disorder (SUD) Information for all HIPAA Covered Entities

November 7, 2025
Bill Seeks HIPAA-Like Protections for Consumer Health Data
Quoted, Bank Info Security

September 24, 2025
The ‘HIPAA-compliant’ myth and other health privacy fallacies
Quoted, STAT+

August 19, 2025
Why Do HIPAA Risk Analyses Miss the Mark So Often?
Quoted, Healthcare Info Security

July 25, 2025
Patients Still Struggle With Full Access to Health Info
Quoted, Healthcare Info Security

June 20, 2025
Court Ditches HIPAA Reproductive Health Info Privacy Rule
Quoted, Healthcare Info Security

June 1, 2025
Manage Third-Party Vendor Relationships Carefully
Quoted, Healthcare Risk Management

April 14, 2025
Using AI in hospitals: the HIPAA hurdle
Quoted, Medical Technology

March 27, 2025
HHS To Cut 10,000 Jobs As RFK Jr. Reorganizes Agency
Quoted, Law360

March 27, 2025
RFK Jr. Cuts at HHS Affect HIPAA, Cyber Response Units
Quoted, Healthcare Info Security

February 25, 2025
A Year After Change Hack, Healthcare Still A Data 'Honeypot'
Quoted, Law360

February 19, 2025
Home-Based Care Providers Vulnerable to HIPAA Compliance Issues
Quoted, Home Health Care News

February 11, 2025
CISA and FDA Sound Alarm on Backdoor Cybersecurity Threat with Patient Monitoring Devices

February 6, 2025
Generative Artificial Intelligence Leveraged to Deliver Healthcare - Legal Risks and Issues

February 2025
OCR Proposes Regulatory Facelift to the HIPAA Security Rule
Co-Author, Houston Medical Times

January 13, 2025
Outlook 2025: Look for MA Cases Based on Claim Denials; Incoming DOJ May Tweak Guidance
Quoted, COSMOS

January 13, 2025
Outlook 2025: Disruption Is Expected, Along With More OIG Guidance, Payment Changes
Quoted, COSMOS

January 6, 2025
OCR Proposes Regulatory Facelift to the HIPAA Security Rule: Addressing the Current Cybersecurity Environment with More Specificity and Additional Requirements

January 2, 2025
What's in HHS' Proposed HIPAA Security Rule Overhaul?
Quoted, Healthcare Info Security

November 26, 2024
Watchdog Report: HHS OCR Should Beef-Up HIPAA Audit Program
Quoted, Bank Info Security

October 23, 2024
Frustrated with Change Healthcare breach, senators propose removing limits on HIPAA fines
Quoted, STAT+

September 17, 2024
Cyberattacks plague health care. Critics call the federal response 'inadequate'
Quoted, NPR

September 5, 2024
RansomHub Claims Theft of Montana Planned Parenthood Data
Quoted, Healthcare Info Security

September 4, 2024
HHS OCR Drops Appeal of Court's Web Tracker Ruling
Quoted, Healthcare Info Security

September 3, 2024
HHS Privacy Loss Not a Green Light for Health-Care Web Tracking
Quoted, Bloomberg Law

July 17, 2024
Court's Web Tracker Ruling: What HIPAA Entities Should Know
Featured, Healthcare Info Security

July 3, 2024
HHS HIPAA Web-Tracking Guidance Takes a Step Back, While Providers Grapple with Latest Challenges

May 13, 2024
HIPAA Privacy Final Rule: Landmark Changes Related to Reproductive Health Care Information

April 2024
HHS Proposes Cybersecurity Requirements for Hospitals
Quoted, Healthcare Risk Management Vol 46, No 4

April 12, 2024
American Privacy Rights Bill: Implications for Health Sector
Quoted, Data Breach Today

March 29, 2024
4 Things You Need to Know About Health Care Cyberattacks
Quoted, The New York Times

March 19, 2024
HHS Tweaks Online-Tracking Guidance After Hospitals' Lawsuit
Quoted, Bloomberg Law

March 19, 2024
Tracker Backtrack? Feds Revise HIPAA Guidance on Web Tools
Quoted, Healthcare Info Security

March 5, 2024
Dissecting Recent Cybersecurity Regulatory Moves at the Federal and State Levels
Featured, AHLA's Speaking of Health Law

February 14, 2024
HHS Finalized Part 2 Revisions: What Has Changed?

February 7, 2024
Bolstering Healthcare Cybersecurity: The Regulatory Outlook
Featured, Healthcare Info Security

February 6, 2024
Medical Center Fined $4.75M in Insider ID Theft Incident
Quoted, Healthcare Info Security

December 15, 2023
Health Privacy Foundations
Presenter, Fundamentals of Privacy Law 2023

December 6, 2023
Biden's October 30, 2023, Executive Order on AI: Key Takeaways for Health Care Stakeholders

November 8, 2023
Hospitals Accuse HHS of Double Standard Amid Pixel Privacy Row
Quoted, Bloomberg Law

October 17, 2023
Private Health Data Still Being Exposed to Big Tech, Report Says
Quoted, Bloomberg Law

October 9, 2023
23andMe Investigating Apparent Credential Stuffing Hack
Quoted, Healthcare Info Security

September 14, 2023
US Senator Seeks Input on Ways to Protect Patient Privacy
Quoted, Healthcare Info Security

September 1, 2023
Employee Curiosity Sometimes Overcomes HIPAA Training
Quoted, Relias Media

June 29, 2023
HHS OIG Releases Final Information Blocking Enforcement Rule Applicable to Non-Provider Actors

May 10, 2023
Proposed Regulatory Oversight on the Emerging Use of Artificial Intelligence in Digital Health

April 13, 2023
HIPAA Notice of Proposed Rulemaking on Reproductive Health Care Privacy

March 7, 2023
FTC Targets Disclosure of Health Data for Web Tracking Again

February 7, 2023
“First-of-Its-Kind” FTC Breach Enforcement Case on Hot-Button Website Tracking Issue

December 15, 2022
Emerging Threats: Cyber Attacks and Side-Channel Evolution

July 13, 2022
HHS OCR Issues New, Post-Dobbs Guidance

February 10, 2015
Latest Update on Anthem Data Breach - Other BCBS Plans May Be Impacted