Shumaker

JANUARY 5, 2026 | PUBLICATION

Client Alert: HIPAA Enforcement Risks and Mitigation Strategies: Summary of Recent Office for Civil Rights Actions

INDUSTRY SECTOR

Health Care

SERVICE LINE

Health Law

RELATED PROFESSIONALS

Grant P. Dearborn

MEDIA CONTACT

Wendy M. Byrne
wbyrne@shumaker.com

This summary highlights recent 2025 Health Insurance Portability and Accountability Act (HIPAA) enforcement actions by the U.S. Department of Health and Human Services' (HHS) Office for Civil Rights (OCR), the risks they underscore for health care organizations and business associates, and practical strategies to mitigate enforcement exposure.

Overview

OCR's recent settlements reinforce consistent enforcement priorities: (i) timely patient Right of Access; (ii) prohibition on impermissible disclosures (including via websites and social media); (iii) foundational Security Rule obligations, especially accurate and thorough risk analysis and risk management; (iv) timely breach notification; and (v) workforce training and policy maintenance. These 2025 settlements have resulted in six-figure settlements and multi-year corrective action plans with monitoring.

Key Themes and Enforcement Focus

OCR emphasized that individuals must receive timely access to records within 30 days (with one allowable 30-day extension) and has advanced its Right of Access Initiative through repeated enforcement, including its 54th action in the Concentra matter. OCR reiterated that posting testimonials or "success stories" with patient health information (PHI) on public-facing websites or social media generally requires a valid, written HIPAA authorization and that such disclosures without authorization constitute impermissible disclosures and potential breaches. Across ransomware and other cyber incidents, OCR found repeated failures to conduct accurate and thorough risk analyses and to implement risk management plans, underscoring that

these are foundational Security Rule obligations. OCR also highlighted timely and complete breach notification as a continuing enforcement focus.

Recent 2025 Enforcement Settlements: Risks and Takeaways

Concentra, Inc.—Right of Access

1. OCR settled alleged Privacy Rule Right of Access violations after determining Concentra failed to provide an individual's PHI within 30 days despite multiple requests; access was ultimately provided more than a year after the initial request. The matter concluded prior to hearing with a $112,500 payment and a settlement agreement. This marked OCR's 54th Right of Access enforcement action. Risk takeaway: failure to meet the 30-day Right of Access standard (plus one possible 30-day extension) is a continuing OCR priority and is likely to trigger investigation and monetary settlement.
2. Cadia Healthcare Facilities—Impermissible Disclosures and Breach Notification
   OCR found that Cadia posted patients' names, photographs, and condition/treatment information as "success stories" on public websites without valid, appropriate written HIPAA authorizations, affecting 150 patients, and failed to provide breach notifications. Cadia agreed to a two-year monitored corrective action plan and paid $182,000, and must revise policies, train workforce (including marketing), and notify all individuals whose PHI was posted without authorization. Risk takeaway: marketing and public-facing communications pose significant Privacy Rule risk; absent valid authorizations, disclosures of PHI in testimonials or social media (including photographs) are likely impermissible and can also trigger breach notification duties.
3. BST & Co. CPAs, LLP (Business Associate)—Security Rule Risk Analysis and Ransomware
   Following a December 2019 ransomware incident, OCR concluded BST failed to conduct an accurate and thorough risk analysis to determine risks and vulnerabilities to ePHI. BST paid $175,000 and agreed to a two-year monitored corrective action plan with OCR. The corrective plan requires a comprehensive risk analysis, risk management plan, policy maintenance, and annual workforce training. OCR recommended sector-wide steps, including asset and data flow mapping, periodic risk analyses, audit controls, user authentication, and encryption at rest and in transit. Risk takeaway: business associates face direct Security Rule enforcement; risk analysis and risk management gaps are prime OCR targets, especially post-ransomware incidents.
4. Syracuse ASC, LLC—Security Rule and Breach Notification in Ransomware
   A ransomware attack affecting 24,891 individuals led OCR to findings that Syracuse ASC never conducted an accurate and thorough risk analysis and failed to timely notify affected individuals and HHS; the entity paid $250,000 and accepted a two-year corrective action plan. Obligations include a formal risk analysis, risk management measures, policy revisions, and annual training; OCR reiterated mitigation steps similar to those described in BST, including audit controls, activity reviews, user authentication, encryption, and lessons-learned integration. Risk takeaway: small and single-facility providers are not exempt from HIPAA Security requirements; failure to conduct risk analyses and to meet breach notification timelines is likely to drive significant enforcement against a facility or provider.
5. Deer Oaks—Privacy/Security Rule, Public Exposure, and Subsequent Network Breach
   OCR substantiated that ePHI from discharge summaries and initial assessments was publicly accessible online due to a coding error in a pilot portal from at least December 2021 to May 19, 2023, affecting 35 individuals. OCR expanded the investigation after an August 29, 2023 network breach impacting 171,871 individuals. OCR found Deer Oaks failed to conduct an accurate and thorough risk analysis and required a two-year corrective action plan and $225,000 payment, including annual risk analysis updates, risk management, policy maintenance, and workforce training. Risk takeaway: configuration and software development errors that expose ePHI publicly are treated as impermissible

disclosures and trigger enforcement; risk analyses must be updated to reflect new risks, technologies, and operational changes.

Comparative Snapshot of Enforcement Outcomes

Entity	Core Violation(s)	Affected Individuals	Payment	Monitoring/Corrective Focus
Concentra	Right of Access failure to provide timely records	Not specified in notice	$112,500	Access compliance; Right of Access priority
Cadia Healthcare	Impermissible disclosures via website; failure to notify	150 individuals	$182,000	Policies, workforce training, notifications
BST (BA)	No accurate/thorough risk analysis; ransomware	Covered entity's PHI impacted	$175,000	Risk analysis/management, policies, training
Syracuse ASC	No risk analysis; late breach notification; ransomware	24,891 individuals	$250,000	Risk analysis/management, policies, training
Deer Oaks	Public exposure of ePHI; later network breach; no risk analysis	35 public exposure; 171,871 breach	$225,000	Annual risk analysis updates, risk management, policies, training

Enforcement Risk Indicators

OCR frequently initiates investigations following complaints about access delays, reports of impermissible disclosures, and breach submissions—including ransomware and public exposure incidents. Common deficiencies include the absence of any risk analysis or failure to update risk analyses when deploying new technologies or expanding operations. For significant or important substantiated violations, multi‑year corrective action plans and required policy updates, training, and monitoring are typical resolution terms, sometimes accompanied by monetary settlements.

Practical Risk Mitigation Strategies

Organizations should institutionalize the Right of Access workflow and track the 30‑day deadline with one possible 30‑day extension, including cost‑based copy fee controls and escalation paths, to avoid access complaints. Marketing and communications teams must be trained that public use of PHI—including names, images, and condition/treatment details—generally requires a valid, written HIPAA authorization and should implement pre‑publication authorization checks and centralized approval. Conduct an accurate and thorough

organization‐wide risk analysis that maps where ePHI is located, how it flows, and how it leaves the environment; refresh this analysis whenever technologies, vendors, or operations change. Implement a risk management plan that prioritizes identified risks with specific controls and timelines and track remediation to completion with governance oversight. Establish and test breach response procedures, including timely individual and HHS notifications, and integrate lessons learned into security management. Strengthen technical safeguards—enable audit controls and regular activity reviews; implement strong user authentication; and encrypt ePHI in transit and at rest where appropriate. Maintain and regularly update written policies and procedures aligned to the Privacy, Security, and Breach Notification Rules and provide role‐based, annual workforce training. For business associates, confirm contractual obligations, conduct identical risk analysis and management, and coordinate incident response and notifications with covered entity clients.

Action Plan for Reduced Enforcement Exposure

Start the New Year with an action plan that includes reviewing your company's HIPAA compliance.. **In the next 60 days**, complete an enterprise‐wide HIPAA risk analysis that documents ePHI systems, data flows, vendors, and vulnerabilities and activate interim controls for critical risks. **In 61–80 days**, adopt a written risk management plan, update security and privacy policies, implement audit logging reviews, enforce strong authentication, and roll out focused training for access, marketing, IT, and compliance personnel. **In 90 days**, run a breach tabletop exercise, validate notification playbooks and timelines, remediate remaining high‐risk items, and embed lessons learned into the security management process. The actions you will take will be affected by the size and sophistication of your company but remember the size of the Syracuse ASC was not a "get out of jail free card."

For more information, please contact Grant Dearborn or another member of Shumaker's Health Law Team.

Shumaker