State Attorney General Health Data Privacy and Security Settlements, 2020-2026

Date announced	Company	Type of organization	Amount (as announced)	Who brought it	People affected	What happened and what the states alleged	Source	Additional source
Nov. 2026	**Perry Johnson & Associates (and four affiliated companies)**	Transcription, coding, and billing vendor (business associate)	Up to $10M announced; $300,000 payable now, $9.7M suspended unless the terms are violated	New York, New Jersey, Connecticut, Michigan	13.3M	March 2023 breach. Hackers used an employee's credentials, and remote access did not require multi-factor authentication. Unencrypted files were accessed, and security software that logged the activity was not set to alert anyone. States alleged HIPAA Security Rule and state law violations, reportedly including an inadequate risk analysis, missing business associate agreements with affiliated firms, and breach notification deficiencies. Required changes include a security program, multi-factor authentication, encryption, annual risk assessments, and independent assessments for three years. Companies neither admit nor deny the findings.	Connecticut AG release	Bank Info Security (ISMG)
Sept. 2026	**Laboratory Corporation of America (Labcorp)**	Clinical laboratory	$2.3M	44 AGs (led by CT, FL, IL, IN, MI, TX)	27.5M in the AMCA breach, including 10.2M Labcorp patients	2019 breach at Labcorp's debt collector, AMCA, exposed patient information. States held Labcorp responsible for the vendor handling its patients' data. The settlement requires stronger safeguards and vendor management and supplements the 2021 AMCA settlement. Labcorp separately agreed to a $35M class action settlement.	Connecticut AG release	Michigan AG release
Oct. 2024	**Albany ENT & Allergy Services**	Physician practice	$2.25M	New York	200,000+	Two cyberattacks compromised the medical records of more than 200,000 patients. The settlement requires stronger security practices, including oversight of information security vendors.	WNY News Now	
Aug. 2024	**Enzo Biochem / Enzo Clinical Labs**	Diagnostic laboratory	$4.5M (NY $2.8M; NJ about $930,000; CT $743,110)	New York, New Jersey, Connecticut	2.4M	April 2023 ransomware attack. Attackers used two employee logins that were shared among five employees, and one had not been changed in 10 years. The company had no process to monitor for suspicious activity. The states alleged HIPAA and state law violations. Neither admitted nor denied.	New York AG release	Enzo Biochem SEC filing
Jan. 2024	**Refuah Health Center**	Community health center	$450,000 in penalties and costs, plus $1.2M required cybersecurity investment	New York	250,000+	May 2021 ransomware attack. The New York AG alleged HIPAA Security Rule, Breach Notification Rule, and New York law violations, including failure to use multi-factor authentication. Refuah must obtain a security assessment within a year and third-party assessments annually for five years.	The Record	HIPAA Journal
Dec. 2023	**Healthplex**	Dental insurer	$400,000	New York	89,955	November 2021 phishing attack on an employee's email account that held more than 12 years of emails. The AG alleged no multi-factor authentication across all Office 365 login routes and no data security assessments. Healthplex must maintain a security program, encrypt data, set an email retention schedule, enforce complex passwords, and conduct penetration tests. No admission of wrongdoing.	HIPAA Journal	Insurance Journal
Oct. 2023	**Inmediata Health Group**	Healthcare clearinghouse	$1.4M	33 AGs (Indiana led)	About 1.5M	Health information was searchable online for almost three years because of a coding issue. The states alleged no secure code review before the breach and notification delayed more than three months, with misaddressed notices. Claims included state consumer protection and breach notification laws and HIPAA. Requires annual third-party security assessments for five years.	Utah AG release	Nebraska AG release
Oct. 2023	**Blackbaud**	Software vendor (customers include healthcare organizations)	$49.5M	50 AGs (Indiana led)	Millions of consumers; 13,000+ customer organizations	2020 ransomware attack exposed Social Security numbers, financial information, and protected health information, among other data. The states alleged violations of state consumer protection laws, breach notification laws, and HIPAA. Requires third-party assessments of compliance for seven years.	Michigan AG release	Nevada AG release
2021	**American Medical Collection Agency (AMCA)**	Medical debt collector (vendor to healthcare providers)	$21M suspended payment (due to bankruptcy)	Multistate coalition of AGs	27.5M	2019 breach exposed personal information of about 27.5M people, including patients of laboratory companies. The coalition settled in 2021 after AMCA's bankruptcy petition was dismissed, and the payment was suspended because of the bankruptcy. The 2026 Labcorp settlement supplements this one.	Colorado AG release	
Sept. 2020	**Anthem**	Health insurer	$39.5M multistate, plus a separate $8.69M with California	43 AGs (Connecticut led)	78.8M	Cyberattack on Anthem's data warehouse, which reportedly began with a phishing email, exposed names, birth dates, Social Security numbers, and health ID numbers. The breach began in 2014 and was disclosed in 2015. Anthem did not admit any violation. Required stronger security and third-party assessments for three years. A class action separately settled for $115M.	North Carolina DOJ release	Bloomberg Law

Patterns across these cases

- Vendors and business associates are frequent targets. Perry Johnson, Blackbaud, Inmediata, and AMCA/Labcorp all involve a company handling data for others. The Labcorp case also shows a covered entity answering for its vendor's breach.
- The same basics keep appearing. No multi-factor authentication, shared or stale credentials, weak monitoring, and late or flawed breach notices show up across these cases.
- The money varies widely. Announced amounts range from $400,000 to $49.5 million, and some, like Perry Johnson and AMCA, are largely suspended. Most settlements also impose multi-year requirements, such as third-party security assessments for 3 to 7 years.
- New York is a repeat player, and often combines HIPAA with its own data security law.

About this document

This list was compiled by The HIPAA E-Tool® from state attorney general press releases and news reports. It is not exhaustive. Amounts and details are as announced; check the linked sources for the full terms. For general information only, not legal advice. Last updated November 11, 2026.