Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10169 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Recent Actions Signal Increased NYDFS Health Cyber Focus

By **Jason Johnson and Linda Malek** (May 29, 2026, 3:15 PM EDT)


Jason Johnson


Linda Malek

On April 29, the New York Department of Financial Services announced the finalization of a $2.25 million settlement with Delta Dental of New York Inc. and Delta Dental Insurance Co., resolving allegations that the affiliated companies failed to comply with the state's stringent cybersecurity, consumer data protection and incident reporting requirements.[1]

For health insurers, managed care organizations and their third-party service providers operating in New York, the announcement comes as the latest signal that the NYDFS intends to aggressively enforce its cybersecurity regulations — which are widely considered the strictest in the nation following a 2023 overhaul.[2]

These regulations, codified at Title 23 of the New York Code of Rules and Regulations, Part 500, apply to any entity licensed under New York insurance law.[3]

This recent development both spotlights the enhanced compliance obligations payors operating in New York state face under the revamped NYDFS regulations and illustrates the importance of proactively developing, enacting and communicating a comprehensive cybersecurity strategy that encompasses:

- A clear data retention policy that ensures timely disposal of plan members' nonpublic information;
- Detailed and actionable guidance for employees in the event of a cyber breach or other incident;
- Instructions for employees to comply with all state-level notice requirements, including disclosures to members and regulators, within statutory deadlines; and
- Risk mitigation strategies and compliance best practices regarding the use of vendor tools and services.

Enforcement in Perspective: Why the Delta Dental Settlement Matters

The Delta Dental investigation arose from a 2023 data breach in which hackers took advantage of a then-unknown flaw in MOVEit, a third-party file tool used by the organization to securely transfer data.

The breach exposed approximately 60,000 files containing sensitive policyholder information, including Social Security numbers, financial details and health records.

Following a NYDFS investigation, regulators contended that the companies lacked adequate data disposal policies, failed to maintain sufficiently detailed incident response plans and did not notify authorities until mid-December 2023 — a date well beyond the rule's required 72-hour reporting window. The matter was ultimately resolved through a consent order requiring a $2.25 million payment. However, the underlying investigation provides invaluable insight into the NYDFS' enforcement strategy and potential compliance risks.[4]

First, it should be noted that the Delta Dental matter is one of two multimillion-dollar resolutions pursued by the NYDFS against healthcare organizations alleged to have violated the state's robust cybersecurity requirements within the last calendar year. In August 2025, the NYDFS **resolved** an action against Healthplex Inc., a dental insurance management services company licensed as an independent adjuster and insurance agent, following allegations that its inadequate cybersecurity protocols — and, in particular, its alleged failure to fully implement multifactor authentication safeguards — contributed to the exposure of customer data after a 2021 phishing attack.[5]

Second, the investigation illustrates that Health Insurance Portability and Accountability Act compliance does not satisfy a payor's full cybersecurity obligations under New York law. The Delta Dental matter focused in part on alleged violations of Section 500.13, which requires covered entities to establish policies and procedures for the secure disposal of nonpublic information that is no longer necessary for business operations.[6] This is a data minimization standard more commonly associated with privacy law than with HIPAA, which focuses primarily on limiting access to and disclosure of data rather than mandating deletion.

Organizations that have built their compliance programs around HIPAA alone may be leaving a significant gap with respect to this deletion obligation — one that the NYDFS appears to be actively closing through enforcement.

Third, it is worth noting that both the Delta Dental and Healthplex matters are among the first enforcement actions brought against healthcare organizations in the period following the amendment of Section 500.

Importantly, however, both enforcement actions were brought under the version of the regulations that predated the November 2023 amendments — meaning even the preamendment obligations are being actively enforced.[7] The final phase of new requirements took effect in November 2025, imposing new obligations regarding multifactor authentication and asset inventory.

Multifactor Authentication

The updated regulations now require multifactor authentication for all individuals accessing any of a covered entity's information systems, applying without distinction as to where a user is located, what role they hold, or what category of data happens to reside on the system in question.

Entities that qualify for the limited exemption under Section 500.19(a) face a narrower but still significant obligation: Multifactor authentication must be in place for remote access to the covered entity's own systems, access to outside applications — including those hosted in the cloud — that handle nonpublic information, and all elevated-privilege accounts, with the exception of service

accounts that do not permit interactive login.

As artificial intelligence tools become more deeply integrated into payor operations, the breadth of this obligation is likely to expand accordingly.

Asset Inventory

Covered entities must now formalize and maintain a formal, well-documented record of all information systems within the organization, supported by written procedures that address how asset details are captured and how often the inventory is reviewed and confirmed as current.

Finally, organizations should be aware that the NYDFS has made clear it will not permit responsibility for cybersecurity compliance to be delegated to vendors.

In an October 2025 guidance, the NYDFS signaled that it will hold covered organizations — defined in Section 500 as "any person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law" — accountable when vendor oversight is inadequate, treating such gaps as relevant considerations in regulatory reviews and disciplinary proceedings.[8]

Implications and Recommendations for Payors

The Delta Dental settlement, taken in conjunction with recent NYDFS communications and the 2025 Healthplex action, makes it clear that the NYDFS views cybersecurity enforcement in the healthcare and insurance sectors as an ongoing priority — and that compliance with the amended Section 500 requirements will be closely scrutinized.

Health insurers and managed care organizations operating in New York should treat these enforcement actions not merely as cautionary tales, but as a road map for the compliance gaps regulators are most likely to target, including data disposal practices, incident response planning, vendor oversight and multifactor authentication implementation.

Proactive engagement with these obligations — rather than reactive remediation following a breach or regulatory inquiry — remains the most effective strategy for managing enforcement risk under New York's increasingly rigorous cybersecurity framework.

Jason Johnson and Linda Malek are partners at Crowell & Moring LLP.

[1] In re: Delta Dental Insurance Co. & Delta Dental of New York, Inc., N.Y. Dep't of Fin. Servs. (Apr. 29, 2026) (consent order).

[2] Cybersecurity, N.Y. Dep't of Fin. Servs., https://www.dfs.ny.gov/industry_guidance/cybersecurity.

[3] Cybersecurity Requirements for Financial Services Companies, N.Y. Comp. Codes R. & Regs. tit. 23, pt.

500 (2023).

[4] In re: Delta Dental Insurance Co., supra note i.

[5] N.Y. Dep't of Fin. Servs., Superintendent Adrienne A. Harris Secures $2 Million Cybersecurity Settlement with Healthplex, Inc. (Aug. 14, 2025), https://www.dfs.ny.gov/reports_and_publications/press_releases/pr20250814.

[6] 23 N.Y.C.R.R. § 500.13.

[7] N.Y. Dep't of Fin. Servs., Cybersecurity Implementation Timeline for Covered Entities (Nov. 1, 2023), https://www.dfs.ny.gov/system/files/documents/2023/11/cybersecurity_implementation_timeline_covered_entities.pdf.

[8] N.Y. Dep't of Fin. Servs., Guidance on Managing Risks Related to Third-Party Service Providers (Oct. 21, 2025), https://www.dfs.ny.gov/industry-guidance/industry-letters/il20251021-guidance-managing-risks-third-party.