akerman

Blog Post

NYDFS Highlights Strategies to Combat AI Cybersecurity Risks

December 2, 2024

By Jordan T. Cohen, Elizabeth F. Hodge, and Ameer Al-Khudari

The increased use of artificial intelligence (AI) in the banking, insurance, and financial services industries has led the New York State Department of Financial Services (NYDFS or Department) to publish an Industry Letter on October 16, 2024, that highlights cybersecurity risks resulting from the use of AI, the dangers posed by threat actors utilizing AI, and strategies to address these concerns (the Guidance).

New York's *Cybersecurity Requirements for Financial Services Companies* regulation at 23 NYCRR Part 500 (Cybersecurity Regulation or Part 500) codifies existing cybersecurity obligations. The new Guidance does not impose additional requirements but instead outlines how the banking, insurance, and financial services companies that NYDFS regulates (Covered Entities) should use the existing framework in Part 500 to address and mitigate AI-related risks.

The new Guidance discussed below raises important considerations for healthcare organizations that are Covered Entities under NYDFS rules, including health maintenance organizations, health insurance companies, third-party administrators, and others.

Cybersecurity Risks From Threat Actors

Related People

Ameer Al-Khudari
Jordan T. Cohen
Elizabeth F. Hodge

Related Work

Data Privacy and Security
Digital Health
Healthcare

Related Offices

Chicago
New York
West Palm Beach

Health Law Rx

Akerman Perspectives on the Latest Developments in Healthcare Law

Read blog posts

In the Guidance, NYDFS highlights several significant cybersecurity concerns originating from malicious actors, including:

- **AI-Enabled Social Engineering.** Highly convincing deepfakes (realistic and interactive audio, video, and/or text) are increasingly used to convince individuals to disclose sensitive information about themselves or their employers, allowing threat actors to gain unauthorized access to information systems and nonpublic information (NPI). Realistic deepfakes can also be used to circumvent biometric verification systems used for logging in to devices and user accounts. Social engineering attacks utilizing deepfakes have also convinced or coerced employees to unknowingly wire substantial amounts of funds to fraudulent accounts.

- **AI-Enhanced Cybersecurity Attacks.** AI can amplify the intensity and success rates of cyberattacks, allowing threat actors to identify and exploit security vulnerabilities far more quickly than humans alone. With AI resources increasingly more available to the public, the barrier to entry for threat actors is lower, which could lead to an increase in the frequency and severity of such attacks.

Cybersecurity Risks of Reliance on AI

NYDFS also highlights risks stemming from Covered Entities' reliance on AI, including:

- **Exposure or Theft of Vast Amounts of NPI.** To develop or deploy AI, Covered Entities collect and process substantial amounts of data, including NPI in large quantities. Storing vast amounts of data creates a greater incentive for threat actors to target these Covered Entities and extract that data. When this stored data includes biometric data, the risk is magnified because threat actors can use such data to bypass multifactor authentication (MFA) to access sensitive accounts and

information or use that biometric data to create deepfakes of individuals.

- **Supply Chain Dependencies.** Implementation of AI often involves third-party vendors and service providers who are also subject to possible attacks from threat actors. The Guidance emphasizes that each link in the supply chain introduces potential vulnerabilities that threat actors can exploit, thereby jeopardizing a Covered Entity's NPI.

Measures and Controls to Mitigate AI-Related Threats

There is no shortcut for assessing and addressing the cybersecurity concerns that AI's proliferation poses. New York's Cybersecurity Regulation, amended in November 2023, requires Covered Entities to assess risks and implement minimum cybersecurity standards to mitigate threats. Additional requirements related to access controls and data management, discussed below, will come into effect in November 2025. In the Guidance, NYDFS addresses the following mitigation and control measures for Covered Entities to reduce AI risk:

- **Risk Assessments and Risk-Based Programs, Policies, Procedures, and Plans.** Covered Entities must incorporate AI-related threats into their risk assessments and ensure they are regularly updating these assessments to reflect identified risks. Proactive response plans to cybersecurity events — which are already a requirement under the Cybersecurity Regulation — should be "reasonably designed" to address AI-related risks.

- **Third-Party Service Provider and Vendor Management.** Thorough due diligence is critical before engaging third-party service providers who will have access to a Covered Entity's information systems or NPI. Covered Entities should assess AI-related risks before contracting with third parties, review contract provisions, and

consider the incorporation of additional representations and warranties in light of AI-related cybersecurity risks.

- **Access Controls.** Considering the threat of increasingly realistic deepfakes discussed above and the upcoming MFA requirement in the Cybersecurity Regulation that goes into effect in November 2025, Covered Entities should reconsider MFA that relies on voice, video, or text and instead consider using digital certificates, physical security keys, or biometric authentication with liveness detection.

- **Cybersecurity Training.** Regular cybersecurity awareness training for all personnel is essential and must address social engineering attacks. NYDFS suggests simulated deepfake attack exercises for personnel. Covered Entities must also provide specifically designed training for cybersecurity personnel.

- **Monitoring.** Covered Entities are required to have monitoring processes in place to quickly identify security vulnerabilities and to ensure they can remediate such vulnerabilities promptly.

- **Data Management.** The severity of cybersecurity events can be minimized by ensuring that unnecessary NPI is culled from data sets and by maintaining data inventories. Covered Entities must also ensure that controls are in place to prevent threat actors from quickly accessing vast amounts of data. Beginning in November 2025, the Cybersecurity Regulations will require minimum standards for the maintenance and updating of data inventories.

In light of NYDFS' Guidance and the new frontier of AI-related cybersecurity concerns, Covered Entities should be proactive by assessing and addressing AI risks, ensuring compliance with the Cybersecurity Regulation's current requirements, and planning ahead for next year's requirements. The Guidance

demonstrates that NYDFS remains active in this space, and it would not be surprising if the Department increases its enforcement of the Cybersecurity Regulation even before the November 2025 obligations take effect. Covered Entities that have yet to implement the Cybersecurity Regulation requirements should consider putting the required policies and procedures in place, creating training programs to ensure compliance by the Covered Entity's personnel, and satisfying other applicable obligations, some of which, such as risk assessments, can be significant undertakings. Akerman's Healthcare Practice Group is equipped to assist Covered Entities in meeting their cybersecurity obligations.
