Insights, News & Events

NY DEPT OF FINANCIAL SERVICES ISSUES GUIDANCE TO COVERED ENTITIES ON OVERSEEING THIRD-PARTY SERVICE PROVIDERS: 4 AREAS OF FOCUS

Insights
Oct 23, 2025

The New York Department of Financial Services (NYDFS) just sent a stark reminder to covered entities (which includes financial institutions, insurance companies, and any other businesses regulated by the NYDFS) that they are responsible for the oversight of their third-party data service providers – and that this oversight is a key element of any data security program. The October 21 guidance from the NYDFS doesn't impose new requirements or obligations on "Covered Entities" they regulate, but instead clarifies their obligations and provides a series of best practices when it comes to managing third-party risk. This Insight explores what you need to know and how to stay compliant.

Why This Matters

Even if NYDFS asserts that the October 21 guidance doesn't create new obligations, it's always important to take note whenever regulatory authorities issue guidance like this. It likely means that the agency is going to increase its scrutiny on the topic in the near future. It also stands to reason that the agency will expect covered businesses to provide evidence of their third-party risk management reviews that line up with the new guidance.

What's Already in Place

Existing NYDFS regulations already impose obligations related to third-party service providers. They require Covered Entities to implement written policies and procedures designed to ensure the security of systems and

Related People

Kate Dedenbach, CIPP/US
Of Counsel
248.901.0301

Jillian Seifrit, CIPP/US
Associate
610.230.6129

data that are accessible to or held by third parties. These policies already must include:

- due diligence and contractual guidelines;
- access controls mechanisms;
- encryption;
- breach notification; and
- assurances regarding the third-party's cybersecurity measures.

New Focus and 4 Key Takeaways

Under this new guidance, NYDFS expects stronger governance focused on four key areas: additional due diligence in selecting third-party service providers, specific contract terms, continuous oversight of third-party service providers as well as their subcontractors, and the termination of the relationship.

Due Diligence

Covered Entities need to pay careful attention when choosing third-party service providers. The guidance discusses classifying the risks posed by the particular third-party service provider as compared to their necessity. Also, when determining risks, Covered Entities should consider the amount and type of access the third-party service provider will have.

The guidance also provides additional information that they should consider when assessing third-party service provider risks:

- **History of the service provider** and whether they have had past security incidents.
- If the service provider has a **strong cybersecurity program**.
- The service provider's **access policy** and how they will access and store the Covered Entity's data.
- If the service provider regularly tests its **incident response plan**.
- How the service provider **monitors its subcontractors**.

Service Focus

Data Protection and Cybersecurity

Privacy and Cyber

Industry Focus

Financial Services

Resource Hubs

U.S. Privacy Hub

Related Offices

New York

- Whether the service provider participates in any **internal or external audits** or can show compliance with industry frameworks such as NIST.

Contract Provisions

The guidance provides a list of specific contract considerations that Covered Entities should include when dealing with third-party service providers, including:

- **Access controls** – require third-party service providers to maintain policies addressing access controls, including limiting access to sensitive data, limiting the number of privileged accounts, reviewing user access rolls, maintaining password policies, and implementing MFA.
- **Encryption** – require third-party service providers to encrypt data at rest and in transit.
- **Notification** – require third-party service providers to notify the Covered Entity as promptly as possible but in no event later than 72 hours after determining that a cybersecurity incident has occurred.
- **Compliance** – require third-party service providers to confirm their compliance with all applicable laws and regulations.
- **Data location and transfers** – while not required under the NYDFS regulations, the guidance suggests businesses should understand where sensitive data will be maintained in order to assess the risk to that data. Additionally, Covered Entities should understand if the data will be stored or accessed internationally.
- **Subcontractors (fourth parties)** – Covered Entities should require their third-party service providers to disclose the use of subcontractors that may have access to the Covered Entities systems or data. The Covered Entity should also have the ability to reject the use of subcontractors if they fail the due diligence process.
- **Data use and return** – restrict the use and sharing of data and ensure that proper steps are taken to return or delete the data at the end of the relationship.
- **Artificial Intelligence** – if the third-party service provider will utilize AI, Covered Entities should include a clause

related to the acceptable use of AI and whether their data can be used to train the AI model.

Monitoring

- The guidance makes clear that Covered Entity's review of third-party service providers does not end at the contracting phase. It is an ongoing review and monitoring of security practices.
- Covered Entities should consider reviewing the third-party service provider's security attestations like SOC2, ISO 27001, penetration testing, and compliance audits.
- If security deficiencies are noted, the Covered Entity should request updates on remediations.

Ending the Relationship

- Businesses should pay careful attention to ensuring that the third-party service provider no longer has any system assess at the end of the service agreement.
- A review of the data maintained by the third-party service provider must also be assessed to determine whether it needs to be retained for any reason, and if so, how it should be returned to the Covered Entity. If the data is no longer needed, the Covered Entity should obtain proof of data deletion.

Conclusion

Fisher Phillips will continue to monitor developments in this area and provide updates as warranted, so make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information direct to your inbox. If you have questions, please contact your Fisher Phillips attorney, the authors of this Insight, any attorney in our New York City office, or any member of our Data Protection and Cybersecurity team or our Privacy and Cyber team.