THIRD PARTY SERVICE PROVIDER/VENDOR RISK ASSESSMENT GUIDE

Understanding the risk of dealing with third party service providers/vendors that have access to your agency's or brokerage's Nonpublic Information (NPI) is critical for your business, from both a compliance and business perspective. This guide covers the requirements set forth under the NY Cyber Regulation (23 NYCRR 500) and may also be considered adequate practices for any agency or brokerage, whether covered by the NY Cyber Regulation or not. If you are not licensed in NY, we recommend reviewing your state's cyber or data security laws (if applicable) to determine if this is compliant.

There are three steps to effectively assessing the risk of third party service providers/vendors.

1. IDENTIFY

First, you must identify which vendors are third party service providers. These are a person or business that:

1. is not an Affiliate of the Covered Entity (your agency) AND
2. provides services to the Covered Entity AND
3. maintains, processes or otherwise is permitted access to NPI through its provision of services to the Covered Entity.

These are some common third party service providers:

- Carriers
- Management system vendor
- Any rating tools you use
- 3rd party policy administrators
- E&S markets
- Data providers
- Brokers and MGAs
- Outsourced call centers
- HR/Payroll/IT companies

These are generally NOT third party service providers:

- Building services/janitorial services
- Advertising/marketing services
- Cable/internet provider
- Tax advisers, CPAs

BEST PRACTICE ALERT!

We strongly recommend that you document and keep records of your third parties, risk assessments, and due diligence. In the event of a breach or audit, this documentation will be invaluable to demonstrating that you followed the appropriate procedures for protecting your customers' data.

Be aware that contracted IT services present a special case. These third party vendors typically have direct access to all agency internal systems with little or no supervision. Outside of serious due diligence, getting in writing that the IT vendor adheres to its own set of security and cybersecurity procedures is reasonable assurance to an agency. Still, in the special case of contracted IT services, it is important to understand their "off-boarding" procedure to ensure departed employees do not retain access to Covered Entity internal networks and NPI due to poor procedures by contracted IT group. In simplest form, this can be addressed via a periodic compliance check/questionnaire.

Last modified: February 4, 2019 10:36 AM

Copyright © 2019 Big I New York

IDENTIFY, CONTINUED

Once you have identified your third party service providers, we recommend you create an inventory (Sample Third Party Service Provider Tracking Template is available). Keep the inventory and responses with your cybersecurity policy. Periodically conduct due diligence on your identified third party service providers and update as additional vendors are added or removed. In the event of an audit or breach, you will need to demonstrate that you have a consistent process and record of due diligence.

2. CONDUCT DUE DILIGENCE

For each third party service provider, you must make a diligent effort to identify the potential cybersecurity risks of doing business with each vendor, and identify and verify the processes and controls the vendor has in place to protect your NPI.

If you are using our template third party service provider cybersecurity policy, you can follow this framework for conducting due diligence, modifying it as you see appropriate. Here are considerations for conducting your due diligence:

WHAT CONSTITUTES SUFFICIENT DUE DILIGENCE?

The NY DFS has not currently set any minimum standards or provided guidelines for conducting due diligence. According to the NY DFS, agencies have significant flexibility to conduct due diligence to the extent they believe is adequate in their best judgment. Big I NY can provide suggestions as to how to conduct due diligence, but ultimately you must decide your level of comfort based on each situation and vendor.

- Begin by reviewing any of the third party service provider's available certifications of compliance with or adherence to national/international or industry standard cyber security practices such as:
  - 23 NYCRR 500 (New York State Cybersecurity Requirements for Financial Services Companies)
  - ISO/IEC 27000 Family of Standards (International Organization for Standardization systematic approach to managing and securing sensitive company information)
  - SOC2/3 and/or SOC for Cybersecurity (Service Organizations Controls for Certified Professional Accountants)
  - NIST 7621r1 (National Institute of Standards and Technology - Small Business Information Security: The Fundamentals)
  - NIST CSF (NIST Cyber Security Framework)
  - OWASP (Open Web Application Security Project)
  - GDPR (European Union General Data Protection Regulation)

The vast majority of large firms or insurers will already adhere to cybersecurity standards or laws that meet or exceed the requirements of existing state regulations, including but not limited to the NY Cybersecurity regulation. If they attest to compliance with the standards, you may reasonably rely upon this to confirm that they have strong cybersecurity protections in place.

***IMPORTANT: If you are licensed in NY and are completing this process as part of compliance with the NY Cybersecurity Regulation, you cannot rely SOLELY on a third party service provider's certificate of compliance with the NY Cyber Regulation. However, you may consider this as part of your due diligence.**

- Ask for certification that a recent (preferably within the previous 12 months) cybersecurity vulnerability assessment/audit of the TPSP's information technology systems and/or relevant applications was conducted by a qualified party. The results of the TPSPs vulnerability assessment should indicate that it presents no vulnerabilities that expose the agency's NPI or violate NY State law or that any such vulnerabilities have since been eliminated.

Last modified: February 4, 2019 10:36 AM

Copyright © 2019 Big I New York

CONDUCT DUE DILIGENCE, CONTINUED

If the third party service provider is able to provide you with a copy of a cybersecurity vulnerability assessment/ audit, either conducted internally or by an outside vendor, you may also rely on this as part of your due diligence.

- Agency review and acceptance of the TPSP's representations and warranties that address the TPSP's cybersecurity policies and procedures relating to the security of the agency's NPI. Such TPSP policies and procedures may include but not be limited to:
  - access controls, including its use of multi-factor authentication, to limit access to relevant information systems and NPI
  - use of encryption to protect NPI at rest and in transit
  - notice to be provided to agency in the event of a cybersecurity event directly impacting the agency's information systems or NPI.
- The agency may use a Third Party Service Provider Questionnaire that addresses the adequacy of the third party vendor's cybersecurity program. A sample Third Party Risk Questionnaire is available from Big I NY).

3. ASSESS AND CATEGORIZE RISK

Once you have identified a vendor as a third party service provider and conducted due diligence, it's time to make a determination as to the level of risk posed by doing business with the third party service provider. There are many ways to conduct a risk assessment, and this is one possible framework.

1. **Consider relevant risk factors**, including (but not limited to)

   - Level of access vendor is granted to NPI
   - Total amount of NPI accessible to the vendor
   - Cybersecurity policies, procedures, and controls of the vendor, including the use of access controls, encryption at rest and in transit, use of multi-factor authentication, certifications and adherence to accepted cyber/data security standards.

2. **Categorize risk**. In your judgment, based on the risk factors you considered, how great is the risk to your agency?

   - **Low risk** (for example a vendor with exceptionally robust cybersecurity practices – a large national insurance carrier, who has passed an independent cybersecurity SOC3 audit and has certified compliance with the NY Cybersecurity Regulation. Or, a vendor who has access to only a small amount of your NPI, or NPI that is of low value.)
   - **Moderate risk** (this generally will include situations that are not clearly low or high risk. For example, dealing with a third party service provider who has good cybersecurity policies and procedures, but holds or has access to a substantial amount of your NPI, therefore meaning that you would experience considerable impact if they were breached.)
   - **High risk** (for example, a newly-launched business software company, who will integrate all of your software --email, customer information, accounting, etc. into one platform. They will house all of your data on their own servers. They assure you they perform frequent internal security checks, but are unwilling to provide you with any documentation. They recently suffered a data breach in which 5,000 customer credit card numbers were stolen.)

Last modified: February 4, 2019 10:36 AM

Copyright © 2019 Big I New York

ASSESS AND CATEGORIZE RISK, CONTINUED

3. **Determine if you will do business with the third party service provider**, and/or under what conditions. This should involve weighing the risk level of a third party service provider against other factors, which may include:

    - The availability of comparable vendors
    - The cost of mitigating the risk of doing business with the vendor
    - The availability of substitute services or lower-risk alternatives.

4. **Document the results of your risk assessment** in your vendor inventory (another good reason to start with an inventory), including any rationale or justification for doing business with a moderate or high risk third party service provider.

GUIDELINES DISCLAIMER

Big I New York is providing this guide solely as a tool to assist agencies and brokerages in assessing their third party service providers and vendors. This guide is not a substitute for agencies and brokerages independently evaluating any business, legal or other issues, and is not a recommendation that a particular course of action be adopted. State security breach notification and privacy laws, coupled with insurance laws and regulations, impose varying requirements on agencies and brokerages. Therefore, it is extremely important for agencies and brokerages to carefully review applicable laws and regulations in all jurisdictions where they do business in structuring their specific security policies. We have worked from the requirements in New York Regulation 23 NYCRR 500 in formulating this guide, because the New York regulation imposes some of the most specific requirements. If specific advice is required or desired, the services of an appropriate, competent professional should be sought. Any agency or brokerage that uses this guide agrees that Big I NY will have no liability for anything related to the use of this tool to assess third party service providers or vendors.

Copyright © 2019 Big I New York