Considerations When Selecting a Vendor

1. Will the vendor have access to information about your firm or clients? If so, what type of information (e.g. sensitive business data (firm or client) or personal identifying information (employees, individual clients, individuals associated with clients or opposing parties, etc.)?

2. What does vendor access look like? Does the firm provide data directly to vendor (paper or electronic)? Does the vendor have access to systems containing the data? Or is data shared/accessed in some other manner?

3. Is the access required for the vendor to perform work? If not, the firm should take steps to limit access to the least amount of information necessary for the vendor to perform its work.

Vendor Due Diligence Questions

All firms should create a vendor due diligence questionnaire tailored to meet the firm's specific needs. Below is a sample of some basic, broadly applicable vendor due diligence questions. The italicized language provides additional insights. The vendor is referred to as "company" below.

1. Does the company hold any certifications or other designations that evidence an understanding of and compliance with industry-recognized cybersecurity standards? If so, please describe each and provide proof of certification/designation. *[There are several data privacy/security certifications or other designations based on various industry standards that businesses can obtain such as HITRUST, PCI, ISO as well as many others. While certification is not necessary for a vendor to prove that it can protect your data, certifications/designations can provide evidence of the level of sophistication or commitment of an organization with respect to data privacy/security.]*

2. Does the company have a Chief Information Security Officer (CISO) or other official responsible for data protection and security? If there is no CISO, identify the title of the individual responsible for data protection and security. *[If the vendor lists the CFO, Director of Facilities, General Counsel or other non-IT person, that is a red flag.]*

3. Does the company carry cyber liability insurance that provides third-party coverage (provides liability protection to clients of the company if the company suffers a breach or cyber-attack)? Provide the coverage details. *[Third party coverage is key. Coverage limits should be at least $1,000,000 although more may be advisable based on the type of data involved.]*

4. Does the company have data protection and security policies and procedures on which it trains employees and enforces compliance? *[If a vendor does not have policies or procedures relating to data protection and security, that is another red flag. Further, having policies without training or compliance enforcement is as good as having no policies at all.]*

5. Does the company perform security awareness training for its workforce members?

6. Does the company have an incident response plan that has been tested at least annually? *[This question and the next question are critical. Even the best prepared vendor can suffer an attack or a breach. You want to be sure that the vendor is equipped to respond in a way that minimizes harm and disruption.]*

Prepared by the Connecticut Bar Association's Cyber Security and Technology Committee, with a special thanks to Dena M. Castricone, DMC Law LLC.

7. Does the company have written disaster recovery and business continuity plans? If so, how often are those plans updated?

8. Has the company performed a cybersecurity risk assessment or undergone penetration testing of its information systems within the last year? If so, has the company implemented recommendations for improvements resulting from the assessment or testing?

9. Has the company experienced a data breach or cybersecurity incident within the last two years? If so, please provide the details.

10. Is the company subject to or does it comply with data privacy and security regulations or guidance (e.g. HIPAA, GLBA, NYDFS, CCPA, GDPR, PCI, NIST etc.)? If so, please identify.

Sample Contract Provisions

The following sample provisions may be helpful to use as a reference when drafting or negotiating contracts with vendors who have significant access to sensitive information. The exact language required, and definition of terms will differ based on each situation. The list of suggested provisions below is not exhaustive. Specific contract needs will depend on the services the vendor provides and the vendor's level of access to important data.

Cyber Liability Insurance: During the term of the Agreement, Vendor shall, at its own expense, maintain and carry in full force and effect, privacy and network security insurance (cyber liability) covering loss arising out of or in connection with unauthorized access, loss or disclosure of personally identifiable information *[add or protected health information for health data]*, in a minimum amount of $1,000,000 per loss.

Notification and Cooperation: In the event of a Data Security Breach affecting Firm Information, Vendor agrees to: (1) provide Firm notice of such incident within 48 hours of discovery; (2) provide reasonable assistance with the Firm's investigation of the incident; and (3) provide all data required for Firm to meet statutory or regulatory obligations related to the Data Security Breach.

Reimbursement of Costs. In the event of a Data Security Breach that affects Firm Information and is caused by the failures of Vendor, its employees or its information systems, Vendor shall reimburse Firm for all reasonable costs Firm may incur in connection with the Data Security Breach including but not limited to: (a) costs related to compliance with applicable data protection laws or regulations, including but not limited to notifications to individuals, reporting obligations, and credit monitoring requirements; (b) expenses associated with engaging a logistics vendor to coordinate notification of and communication with affected individuals; and (c) expenses, judgments, penalties, fines and settlement amounts actually paid and costs reasonably incurred by Firm in responding to claims or governmental inquiries as a result of the Data Security Breach. The obligations herein shall not be subject to any limitation on liability provisions in this or any other agreement between the parties.

Data Ownership, Return and Destruction. All ownership, title, licenses, proprietary rights and interest ("Title") in Firm Information submitted by Firm to Vendor in connection with the Services is and shall always remain vested in Firm. Nothing in this Agreement confers Title in Firm Information to Vendor in

Prepared by the Connecticut Bar Association's Cyber Security and Technology Committee, with a special thanks to Dena M. Castricone, DMC Law LLC.

any respect. At no cost to Firm and within fifteen (15) days of receiving a written request from Firm, Vendor shall have an absolute obligation to: (1) return the Firm Information to Firm in a format that is acceptable to the parties; and (2) permanently delete all Firm Information in a manner that renders retrieval of the data impossible and certify such deletion. *[Use this provision if firm is providing firm data, such as electronic files, to a vendor]*

Use of Subcontractors. To the extent that Vendor uses subcontractors to deliver Services to Firm, Vendor agrees that it shall be responsible for the acts or omissions of its subcontractors and shall ensure that such subcontractors adhere to the terms of this Agreement.

No Off-Shore Data Transfers. Vendor shall not transfer any Firm Information or perform any processing of Firm Information outside of the continental United States for any purpose. *[Use this provision if firm is providing firm data, such as electronic files, to a vendor. This will be necessary to avoid triggering any data privacy laws in other countries that may not otherwise apply.]*