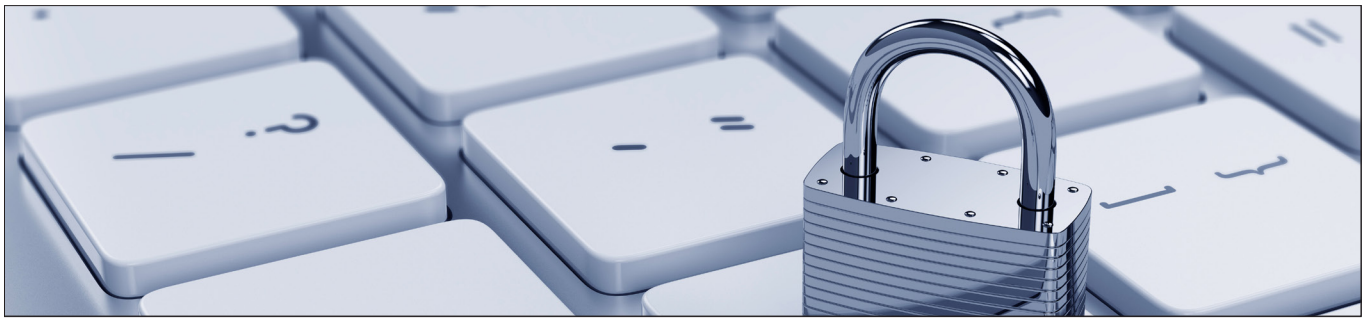
MURTHA CULLINA

NEWS ALERT

INFORMATION SECURITY & HEALTH CARE



Protecting Data: Vendors May Be Your Weakest Link

By Dena M. Castricone and Daniel J. Kagan | July 18, 2017

Just last week, a Verizon Communications vendor misconfigured a cloud server that caused the information of 6 million Verizon customers to be exposed on-line. When a cyber incident or data breach occurs on your vendor's watch, regardless of fault, you own the resulting legal obligations and costs. The best tools for managing the risk of using vendors are due diligence and adequate contract provisions.

Before engaging a vendor, you should consider the vendor's ability to protect your information. One way to accomplish this is to create a vendor security checklist or questionnaire that all potential vendors must complete. For example, you could ask for: (1) a description of security measures in place to protect the information; (2) proof of a third-party risk assessment of its systems; (3) confirmation of adequate training of employees on the protection of data; (4) a history of security incidents over the past three years; and (5) proof of cyber risk coverage. Of course, the depth and detail of the inquiry will depend on the work that the potential vendor would perform. It is important to engage your IT professionals in this process to ensure that you are asking the appropriate questions with respect to technical issues.

Notably, vendor due diligence measures are required by New York's Cybersecurity regulations and will be required by the EU's General Data Protection Regulation when it takes effect in May 2018. And while not required by law in many other settings, vendor due diligence is quickly becoming a standard and expected business practice.

After the due diligence phase, you should ensure that the service contract contains important provisions. The following are examples of such provisions.

- **Required Security Measures:** The contract should detail the security measures that you will require the vendor to implement. Be specific, while leaving open the option that new requirements may emerge, and reserve the right to periodically confirm that the vendor is in compliance. Again, engage your IT professionals.
- **Immediate Notice:** This provision will require the vendor to provide you with notice within a very short time frame in the event of a security incident. Be sure to define "immediate." Twenty-four hours is ideal but three to five business days may also be acceptable.

Dena M. Castricone
Chair, Information Security & Privacy Group
203.772.7767
dcastricone@murthalaw.com

Burt Cohen
Vice Chair, Information Security & Privacy Group
203.772.7714
bcohen@murthalaw.com

Paul E. Knag
Co-Chair, Health Care Group
203.653.5407
pknag@murthalaw.com

Stephanie S. Sobkowiak
Co-Chair, Health Care Group
203.772.7782
ssobkowiak@murthalaw.com

- **Indemnification:** The contract must have a strong indemnification provision that requires the vendor to cover all costs and expenses that flow from any security incident or breach of information it maintained, accessed or promised to secure on your behalf, including notification and reporting costs, legal fees, governmental fines and the cost of any litigation or claim brought against you relating to the security incident or breach.

For health care providers, vendors with access to protected health information must also enter into a business associate agreement ("BAA") under HIPAA. Your standard BAA should address the above provisions. If possible, avoid signing a vendor's standard BAA because it likely will not protect your best interests.

If your entity experiences a breach or if you have any questions about data breaches or any other health law issue, please contact Dena M. Castricone, Daniel J. Kagan or Stephanie S. Sobkowiak.

Dena M. Castricone at 203.772.7767 or dcastricone@murthalaw.com
Daniel J. Kagan at 203.772.7726 or dkagan@murthalaw.com
Stephanie S. Sobkowiak at 203.772.7782 or ssobkowiak@murthalaw.com