TEN DATA SECURITY QUESTIONS TO ASK YOUR VENDORS

1. **What security measures do you use for your company and your data, and will you show me the certifications?**
   You are looking for specifics from your vendors. For example, a vendor stating that it is "SOX certified" is not enough – there are several different levels of SOX certification that they may have, and they may not meet your needs. If you do not know which specifics are important to protect your data, it may be worth hiring a consultant to analyze their security. Ask the vendors to provide proof about such claims. If they balk, chances are they are hiding something.

2. **Where are you storing my data geographically?**
   If there is a breach at a facility in another state or country, you may be subject to that jurisdiction's data breach and privacy laws. Consider writing into any agreement that that data, even the "backup" and "catastrophic recovery" versions, must stay in the United States.

3. **Where are you storing my data in your infrastructure?**
   For any data that is being housed with a vendor, you should have an understanding of the security controls in your vendor's environment and you should insist that they include tightly prescriptive controls around isolation and protection.

4. **How do you notify clients of known security vulnerabilities?**
   It is the policy of some vendors not to disclose a security vulnerability unless it is dangerous to a client's data. This, however, should be your decision to make. Ask what constitutes a "serious" vulnerability and ask about how they categorize risks and security issues. Also ask them about frequency and form of notification because these could impact your business.

5. **Will you be willing to set up regular audits with my company (or provide me with copies of a recent third-party external audit)?**
   Companies that undergo an external audit – either from you or from a third party – have foundational security framework in place and an acceptable baseline of security can be expected. A less-than-scrupulous vendor may claim to have undergone extensive auditing while actually an auditor hadn't come within 10 square miles of their business. A transparent company will have no qualms in granting you those results.

6. **Do you have data security/cybersecurity insurance?**
   No security vendor assumes the risk of a full security breach. They do, however, provide service-level agreements and other services to mitigate risk. Any outsourcing negotiation should include protocol and definition of whom assumes risk in these situations. Get a copy of the policy! This is no different from asking if they have fire insurance and property insurance; it makes the vendor a better partner.

7. **How do you transfer data?**
   The best security in the world is worthless if it is being transferred in an unsecured manner between locations or between you and your vendor. Make sure that the vendor has end-to-end encryption.

8. **Do you follow secure data destruction processes for confidential data and IT equipment/media?**
   If the vendor does not properly destroy data from decommissioned equipment, the data is needlessly put at risk. Ask your vendor about their data destruction process.

9. **For companies with protected health information: will you sign a business associate agreement?**
   If you deal with HIPAA-protected information, your vendors are your greatest liability and, in most circumstances, they must sign a business associate agreement in order for you to be in compliance with HIPAA. If the vendor declines, find another vendor.

10. **What is my ability to get out of the contract, and how will you return my data?**
    Eventually, many relationships end. Vendors naturally try to lock clients into long-term engagements. Consider a shorter-term agreement that can be regularly evaluated and changed to your liking. Make sure you have provisions regarding the return of data, and make sure that the return is not contingent on settling any billing disputes.

Stradley Ronon partners with top providers to offer comprehensive data security solutions for its clients, including information governance policies, advice on HIPAA guidelines, technology audits, and data breach management. Please contact Jana Landon (jlandon@stradley.com) or Jeffrey D. Grossman (jgrossman@stradley.com) for additional information.