TEN DATA SECURITY QUESTIONS TO ASK YOUR VENDORS

1. **What policies and procedures do you use for your company and your data? What certifications do you hold?**

   You are looking for a list of specific policies and procedures from your vendors, as well as a list of specific certifications that are consistent with your organization's needs. For example, a vendor stating that it is "SOX certified" is not enough – there are several different levels of SOX certification; its particular certification may not meet your needs. Ask the vendors to provide proof about any assertions as to policies and/or certifications. If they balk, chances are good that 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 data, even "backup" and "catastrophic recovery," 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 impacts a particular client's data. 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. We recommend that any suspected or actual unauthorized access at the vendor be reported to a designated contact person in your organization within 24 hours and that the vendor be required contractually to cooperate with you to investigate and remediate the breach if it affected your data.

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)?**

   Any vendor should be willing to let you inspect its facility, records and practices as they relate to security. If the vendor is accessing or storing crucial information, consider annual audits.

6. **Do you have data security/cyber liability insurance?**

   Most vendors have some form of professional liability insurance that will protect them during a data breach, but it will probably not protect you. Consider requiring your vendor to obtain cyber liability insurance with a minimum coverage level of $10,000,000. You also want to obtain a copy of their insurance certificate. Also, consider requesting to be named an additional insured under the policy.

7. **How do you store and transfer data?**

   The best security in the world is worthless if it is being transferred in an unsecure manner. Make sure that the vendor has end-to-end encryption for file transfers. Also, consider requesting that your information be encrypted at rest. This would include information on the vendor's systems and storage devices such as USB drives, servers and backup tapes. Encryption keys should be stored in a separate location away from encrypted files.

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 ("BAA")?**

   If you deal with HIPAA-protected information, your vendors are your greatest liability and, in most circumstances, they must sign a BAA 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, delete or destroy my data?**

    Understandably, vendors often want to lock clients into long-term engagements. Consider a shorter-term agreement that can be regularly evaluated and changed to suit your business purposes. In general, vendors should only store data for as long as you specify, or as necessary to satisfy the purposes for which it was provided to the vendor (barring, of course, any applicable time periods contained in laws, regulations, or professional ethics rules). Make sure you have provisions regarding the return, deletion, or destruction of your data, and make sure such action 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.