U.S. Legal Support

9 ESSENTIAL CYBERSECURITY QUESTIONS TO ASK

in the Age of COVID-19 and Beyond

How secure is your case and client data?

Cyber threats are very real. According to a 2016 study[1], over 3 million records are compromised every day, roughly 44 records every second. With increased online activity due to the onset of COVID-19, hacking attempts and breaches continue to become more prevalent. In fact, the FBI has reported[2] a 300% increase in cybercrimes. With the average breach costing businesses $3.9 million[3] per incident, you cannot afford to leave your case and client data unprotected.

To safeguard your confidential information, you need to be aware of potential vulnerabilities so you can take the necessary measures to mitigate risks. When selecting a litigation support services partner for court reporting, record retrieval or other litigation support services, it's essential to thoroughly vet their cybersecurity and data privacy policies. Not only should they have robust plans in place to prevent breaches, they should have plans to respond promptly to any threats that may arise.

Here are 9 essential questions we recommend asking any potential service provider, including helpful information regarding best practices:

1. IS YOUR COMPANY HIPAA COMPLIANT?

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 dictates how protected health information is stored, handled and disclosed. To ensure the confidentiality of your clients' Protected Health Information (PHI), you need to work with a HIPAA compliant partner.

☐

2. HAS A SOC 2 TYPE II AUDIT BEEN CONDUCTED?

SOC refers to "System and Organization Controls" designed to measure how well an organization manages and protects client data. A successful SOC 2 Type II audit takes this an important step farther, confirming that an independent third-party auditor has verified that best-in-class procedures, safeguards and technologies are employed across the five trust principles - security, availability, processing integrity, confidentiality and privacy.

☐

3. HAS AN INDEPENDENT AUDITOR VERIFIED BOTH HIPAA COMPLIANCE AND SOC 2 TYPE II CERTIFICATION?

It is not enough for a vendor to make unverified claims about HIPAA or SOC 2 Type II compliance. Without attestation from a reputable independent auditor, you cannot guarantee that systems and operational processes actually ensure HIPAA compliance and follow SOC 2 Type II guidelines.

Without this third-party verification, a vendor will also be unable to corroborate its answers to the vital questions on this list, including the nature of system and operational controls employed within the company, what risks are being mitigated by these systems and the effectiveness of the controls.

☐

4. DO YOU HAVE A SECURITY OPERATIONS CENTER (SOC)?

A Security Operations Center (SOC) gathers input from the following sources to take action to protect systems and data:

- Intrusion detection and prevention systems that continuously monitor a network for vulnerabilities
- Firewalls that are preventing malicious access to systems
- System events on servers and staff computers that could signal malicious activity

☐

[1] Thales Group. *Breach Level Index*. March 2017.
[2] Tonya Ugoretz, Deputy Assistant Director, FBI. April 2020. Internet Crime Compliant Center.
[3] Larry Ponemon. *2019 Cost of a Data Breach Report.* July 2019. Ponemon Institute.

5. WHAT IS YOUR DISASTER RECOVERY PLAN AND WHAT REDUNDANCIES DO YOU HAVE IN PLACE?

As the saying goes, "if you fail to plan, you plan to fail." Disasters come in many forms. Whether hackers, electrical fires, floods or broken air conditioning units, it's imperative your partner of choice has a disaster recovery plan. Not only does this protect your data, but enables your business to continue operations in the event of an emergency or disaster.

6. HOW IS DATA PRIVACY ENFORCED AND MONITORED?

To safeguard your privacy, a partner should offer strict role-based access control, limiting who has access to your data within the organization. The enforcement of strict access control should be audited and tested in a company's SOC 2 Type II report.

7. WHAT IS THE INCIDENT RESPONSE PLAN?

In the event of a breach, having a complete incident response plan will reduce damage and help you recover as quickly as possible. When considering a potential partner, this is an important component that should not be overlooked. The incident response plan, and how incidents are actually handled in a company, will be audited and tested in the company's SOC 2 Type II report.

8. IS YOUR DATA BACKED UP AND IF SO, HOW OFTEN?

To prevent data loss, a provider should perform at minimum daily backups of all systems and data. A company should also replicate systems and data to a separate geographic location to assure that they are always available. Backup activities should be audited and tested in a company's SOC 2 Type II report.

9. ARE THIRD-PARTY PENETRATION TESTS CONDUCTED ON KEY SYSTEMS EXPOSED TO THE INTERNET TO ENSURE THEY ARE SECURE?

Penetration testing conducted by a reputable third-party firm helps ensure that client data is safe when using systems exposed to the Internet. Confirmation of penetration testing should be included in a company's SOC 2 Type II report and a company should be able to produce a report that shows testing results.

THE U.S. LEGAL SUPPORT DIFFERENCE: Industry Leading Full-Spectrum Security

U.S. Legal Support offers security and data protection that no other litigation support company can provide. We follow the NIST Cybersecurity Framework regarding policies, procedures and controls, meeting and exceeding requirements. We work hard so you can rest easy.

- HIPAA compliant
- SOC 2 Type II certified
- Attestation from reputable independent auditor of all systems, processes and controls
- 24/7 Network and Security Operations Center
- Intrusion detection and prevention systems
- Third-party penetration testing
- Incident response plan that is audited and tested in our SOC 2 Type II report
- Frequent backups and replication across multiple datacenters in separate geographic locations
- Disaster recovery plan

To learn more about our robust security or full-service litigation support services, please contact your local U.S. Legal Support Representative or email hello@uslegalsupport.com.