U.S. Legal Support

UNPARALLELED SECURITY FROM U.S. LEGAL SUPPORT

When it comes to litigating in a pandemic and beyond, cybersecurity should be top of mind.

36% of law firms in an American Bar Association report say they've had malware infections in their systems.[1]

29% of law firms have reported a security breach.[1]

Data breaches in first half of 2021 exposed an estimated 18.8 billion sensitive records.[2]

The total number of security breaches increased by 17% alone in 2021.[3]

Cybersecurity threats are not only growing more prevalent, but also more expensive.

In 2021, the average cost of a data breach reached $4.24 million per incident, the highest in 17 years.[4]

$40 million paid in March 2021 by one of the biggest insurance companies in the world to ransomware hackers to return stolen data.[5]

At U.S. Legal Support, we understand how important it is to keep sensitive case and client information safe and secure. Therefore, we offer cutting-edge security across all facets of our business.

PERSONAL SECURITY TIPS

DO use a secure connection to ensure encryption of data when accessing business applications or services over the internet.

DON'T use a computer in an accessible place in your home or public space where other may see what is on the screen.

DON'T have business phone calls to discuss clients, cases or colleagues where anyone can overhear confidential information.

1. American Bar Association, 2020 Cyber Security, https://www.americanbar.org/groups/law_practice/publications/techreport/2020/cybersecurity/
2. Risk Based Security, 2021 Mid-Year Report, https://pages.riskbasedsecurity.com/download-the-2021-mid-year-data-breach-quickview-report-today
3. Identity Theft Resource Center, https://www.idtheftcenter.org/identity-theft-resource-center-to-share-latest-data-breach-analysis-with-u-s-senate-commerce-committee-number-of-data-breaches-in-2021-surpasses-all-of-2020/
4. IBM REPORT, https://newsroom.ibm.com/2021-07-28-IBM-Report-Cost-of-a-Data-Breach-Hits-Record-High-During-Pandemic
5. https://www.bloomberg.com/news/articles/2021-05-20/cna-financial-paid-40-million-in-ransom-after-march-cyberattack

SECURITY THROUGHOUT ALL DATA CENTERS AND FACILITIES SOC 2 TYPE 2

- An independent auditor has verified the procedures, safeguards, and technology that we employ to ensure the protection of your sensitive data
- Independently examined and verified to be fully HIPAA compliant for the protection, privacy, security, and integrity of all protected health information
- NIST Cybersecurity Framework in place regarding our policies, procedures, and controls
- End-to-end encryption for all transmitted files

HIPAA COMPLIANT

SOC 2 TYPE 2 COMPLIANCE

END-TO-END ENCRYPTION

NIST CYBERSECURITY FRAMEWORK

In addition to these industry-leading security measures, U.S. Legal Support also boosts our security protocols with:

- Attestation from reputable independent auditors of all systems, processes, and controls
- Intrusion detection and prevention systems
- Third-party penetration testing
- An Incident Response Plan vetted by independent cybersecurity incident response experts
- Frequent backups and replication across multiple, geographically dispersed data centers
- Disaster recovery plan