Caplinked™

Enterprise Grade Security

ISO 27001 Certified

CapLinked protects your data both digitally and physically under the strictest international standards and accreditations. All CapLined information is securely hosted on ISO 27001 certified servers to ensure security, availability and privacy of your data.

AICPA SOC 2 Certified

Compliant with international Service Organization Controls (SOC) standards for the secure handling of financial information within a service organization. Assessed in accordance with the SOC Security Principles including organization, communications, risk management, control monitoring, physical data access, system operations, & change management.

EU-US Privacy Shield Certified

CapLinked is certified and complies with the EU-U.S. Privacy Shield Program ("Privacy Shield") framework and its principles as set forth by the US Department of Commerce and the European Commission regarding the collection, use, and retention of data from EU member states.

HIPAA Compliant

CapLinked meets the obligations required by HIPAA, HITECH, and the final HIPAA Omnibus ruling. CapLinked also supports the ability to sign HIPAA Business Associate Agreements (BAAs) with enterprise customers.

PCI SAQ-D Compliant

The servers CapLinked employs are accredited by the Payment Card Industry (PCI) Data Security Standard (DSS). PCI certification is required for any organization that processes credit card payments, and designed to prevent credit card fraud through increased controls around data and its exposure to compromise.

FISMA Compliant

CapLinked enables US government agencies to achieve and sustain compliance with the Federal Information Security Management Act (FISMA). CapLinked achieves FISMA compliance by meeting the controls identified in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev. 4.

The General Data Protection Regulation (GDPR) is an important piece of legislation that is designed to strengthen and unify data protection laws for all individuals within the European Union.

At CapLinked, we are committed to helping our customers fulfill all GDPR requirements.

Caplinked™

World-class data encryption

Secure Connection: All data on CapLinked, whether inbound, outbound, or at-rest, is connected using HTTPS.

256-bit Advanced Encryption Standard: CapLinked encrypts your sensitive data at rest using the strongest block ciphers available and the industry standard.

Premium-Grade TLS Protocol: Your data is encrypted in transit via SSL/TLS-encrypted endpoints using the most up to date TLS v1.2 cipher suites.

Security features and highlights

Secure connection

No plug-ins

CapLinked requires no software plug-ins or updates, such as Adobe Flash, Silverlight, .NET, and Java.

Multi-layer Security Firewalls

CapLinked data is stored behind network segmented firewalls at every point of transit to prevent, protect, and detect external threats.

Real-Time Virus Protection

CapLinked's built in real-time scanning engine protects your users from trojans, viruses, malware & other malicious threats.

Secure storage and hosting

SOC2 Type II certified

CapLinked is SOC2 Type II certified under SSAE 16 (formerly SAS70) and all data is hosted and managed by Amazon Web Services (AWS) via their secure data centers. CapLinked is also PCI SAQ-D compliant and a Cloud Security Alliance member.

Hosted via Amazon Web Services

Secure data centers protect your information both digitally and physically with industry-leading reliability. Amazon Web Service accreditations include ISO 27001, SOC2/SSAE 16/ISAE 3402 (Previously SAS70 Type II), PCI SAQ-D, FISMA Moderate, and Sarbanes-Oxley (SOX).

Amazon OpsWorks

Amazon OpsWorks provides enhanced reliability and security with daily backups, malware mitigation, Safe Harbor certification, and 99.9% uptime.