CRASHPLANPRO™
Continuous Backup for Business

CrashPlan PRO Compliance

CrashPlan PRO aligns with your compliance strategy

Customers expect their service providers to demonstrate that they have adequate controls and safeguards when they host or process data. Compliance with numerous regulations ensures that a provider can demonstrate the required controls and protection. Specifically, CrashPlan is compliant with regulations that prescribe data privacy, its safekeeping and availability.

For additional information about CrashPlan PRO security, please ask for our Security Overview document. It provides additional technical details about CrashPlan PRO security. A summary of this document appears on the next page.

Compliant Regulations

CrashPlan is SAS 70, HIPAA and EU Safe Harbor compliant.*

SAS-70

Statement on Auditing Standards (SAS) No. 70, Service Organizations, is a widely recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). In addition, the requirements of Section 404 of the Sarbanes-Oxley Act of 2002 make SAS 70 audit reports even more important to the process of reporting on the effectiveness of internal control over financial reporting.

CrashPlan PRO has completed the necessary audits and can provide supporting documentation to demonstrate that it is SAS-70 compliant.

HIPAA (Health Insurance Portability and Accountability Act)

HIPAA is the United States Health Insurance Portability and Accountability Act of 1996. This regulatory standard seeks to establish standardized mechanisms for electronic data interchange (EDI), security, and confidentiality of all healthcare-related data.

While there is no official "HIPAA Certificate of Compliance" for backup software and services, installing and implementing a backup strategy with CrashPlan PRO can help customers comply with HIPAA security and privacy rules.

EU Safe Harbor

The European Commission's Directive on Data Protection went into effect in October of 1998, and prohibits the transfer of personal data to non-European Union nations that do not meet the European "adequacy" standard for privacy protection. While the United States and the European Union share the goal of enhancing privacy protection for their citizens, the United States takes a different approach to privacy from that taken by the European Union.

* certification pending. Contact kris@code42.com for more information.

CrashPlan PRO Security

CrashPlan PRO addresses regulatory data security and privacy concerns by employing a multi-layered security model that includes: transmission security, account security (access), password security, encryption security, secure messaging.

Technology

CrashPlan PRO Client and Server execute within the confines of a secure Java virtual machine. All cryptographic functions rely on the industry standard Cryptographic Extensions (JCE) provided therein.

Account Security

All CrashPlan PRO customers have a CrashPlan account, which uniquely identifies them in the CrashPlan database. Within an account, users are assigned roles as a means to limit and control account access.

Password Security

The account password is never stored or transmitted to the CrashPlan PRO Server in plain text.

Encryption Key Security

Backup data is encrypted with a 448-bit data key. This key is typically escrowed in the CrashPlan PRO Server allowing administrators to easily restore and decrypt data on behalf of a user..

- Keys are created using a secure random number generated from Sun Microsystem's Java Cryptography Extensions framework.
- The key used to backup data is stored, just like the data itself, locally on the computer itself in an unsecured location.
- Keys are escrowed within CrashPlan PRO Server and optionally in each backup archive (encrypted) at the destination.

Security Highlights

Multi-layered security

Unique cryptographic keys per user, machine and organizational unit

Secured 128, 256 or 448-bit file encryption

Secured 256-bit AES communication encryption with unique session keys

Flexible key escrow policy

Open-sourced symmetric cipher (Blowfish)

Secure globally unique identifiers

Logged and audit-able restores

Integrates with existing enterprise identity management systems

Automated data retention policies and lifecycles

Tamper-proof backup archives

Centralized administration and event logging

Flexible policy management and stringent enforcement

A Word from Legal...

While CrashPlan PRO meets the technical aspects of information systems regulatory compliance to the best of our understanding, full compliance typically requires deploying administrative procedures and physical safeguards in addition to electronic data security and retention. Because many requirements are beyond the scope of features a backup solution provides, we cannot tell you whether simply implementing a CrashPlan PRO will put your organization in compliance.

For more information about compliance, contact your legal counsel.