Code42 is predicated on two beliefs: first, we believe our customers should benefit from cloud solutions without compromising their data security, regulatory or privacy requirements; and secondly, the customer—not the provider—should decide how a cloud solution is deployed.

We don’t demand blind trust from our customers—our cloud solutions and multi-layered security offering are engineered to give our customers choices in how they mitigate risk and meet their data security, regulatory or privacy requirements.

**Security Personnel**
Code42’s dedicated security team upholds security principles and development ideology, and is responsible for maintaining strict adherence to our Information Security Management System (ISMS) policies. Code42’s cloud security and engineering teams are responsible for self-administered and regular, third-party penetration tests of our cloud data centers; and for annual secure-coding practices reviews.

**Cloud Engineering**
Code42 maintains complete, operational ownership and monitoring of network, systems, applications and security at all of our global data centers. The cloud engineering team continuously monitors system health, secure data transmission, protection from denial of service, and other network and system vulnerabilities.

**Compliance and Legal**
Code42’s compliance and legal team investigates and assures adherence to regulatory obligations and contractual commitments with customers.

**Engineering and Product Development**
All software programming, code development, engineering and quality assurance (QA) is performed by the Code42 team. The Code42 development team follows security standards outlined by the Open Web Application Security Project (OWASP)—and includes code reviews focused on secure transmission and storage of data, initial mapping and analysis of an application’s attack surface, and finding and exploiting security vulnerabilities.

**Principles of Product Development**
Code42 product development is guided by four principles in which no attribute compromises the principle preceding it. These guiding principles are known at Code42 as “SRUP.”

- **S** Code 42 products must be secure.
- **R** Code 42 products must be reliable.
- **U** Code 42 products must be user-friendly.
- **P** Code 42 products must be high-performing (flexible, scalable and fast).
Public Cloud Data Security
Unlike many software vendors offering cloud storage, Code42 does not outsource important components of our cloud stack to third-party, public-cloud providers; we’re our own hosting provider. We own the complete cloud stack comprised of software, server, storage, network, monitoring and security components—and contain them in Code42-provided and controlled racks in all data center locations. As a result, Code42 customers maintain low total cost of ownership without sacrificing high functionality.

Code42 ensures and monitors appropriate ISO27001 or SSAE16 certifications for its cloud data centers, and is an ISO27001-certified organization. Code42 continually strives to keep pace with evolving industry security standards. (See also page 4)

Code42 supports multi-destination backup and provides second destination backup that is completely separate from the primary source.

With Code42, customers are assured that:

- Data stays in the location the customer intended and is compliant with data export laws. It is not replicated to any other location without the knowledge of the customer.

- All data is encrypted at the source, transmitted in an encrypted tunnel and encrypted at-rest. Decryption is strictly controlled by authorized, authenticated customer access.

- As mandated under Health Insurance Portability and Accountability Act (HIPAA), whenever a contract is awarded where the contractor provides functions, activities or services involving the use and/or disclosure of protected health information (PHI), Code42 can execute Business Associate Agreements (BAA) and provide guidance on deploying our software in a HIPAA-supported manner.

- Code42’s secure cloud deployments enable archive encryption key storage on-premises (i.e., private passwords are stored at the customer’s location), not in Code42’s data center. Privately held encryption keys render data completely useless in the event of a security breach during transmission or storage within Code42 data centers.

- Code42 properly and permanently destroys data once an account is deactivated and purged.

Code42 complies with the US-EU Safe Harbor and US-Swiss Safe Harbor Frameworks set forth by the Dept. of Commerce regarding collection, use and retention of personal data from EU member countries and Switzerland.

Code42 has certified that it adheres to the Safe Harbor Privacy Principles of notice, choice, onward transfer, security, data integrity, access and enforcement.

Visit www.code42.com/privacy and www.export.gov/safeharbor
Public Cloud Deployment
Code42 offers public cloud deployments with unique security features needed by business customers. Fully managed, on-premises, master-authentication servers allow businesses to enclose the entire application-authority space privately behind corporate firewalls. This approach enables fully automated directory services integration for real-time enterprise access and permissions synchronization via Active Directory/Single Sign-On, as well as private escrow of encryption keys. As such, all data is de-duplicated and encrypted at the source device (before transmission) and can never be decrypted by anyone—including Code42—without authenticated and authorized access to the encryption keys stored in the master server.

Code42-managed data centers are currently located in the United States in Atlanta, Ga.; Minneapolis, Minn. Quincy, Wash.; and internationally in Dublin, Singapore, Sydney and Tokyo. Additional locations may be added as global demand arises.

Private, On-Premises Cloud Deployments
Code42 offers customers secure, high-performance, scalable and reliable on-premises cloud deployments.

- Code42’s Managed Private Cloud
  Code42’s Managed Private Cloud (MPC) is a turnkey cloud offering that resides in a private customer location.

  Designed and developed by Code42 engineers, MPC appliances remain on the customer site, behind the firewall. The service “calls home” to a central operations center where it is managed and monitored 24 x 7 x 365 by the Code42 Customer Champion support team. Because a managed private cloud keeps keys and data storage completely on-premises, this
deployment supports most data security and compliance requirements. It allows customers to deploy a solution that meets regulatory requirements such as International Traffic in Arms Regulations (ITAR), U.S. Export Controls and HIPAA, among others.

- **Private Cloud**
  Alternatively, customers can also deploy a private cloud by running Code42 software on their own hardware, and managing the service themselves.

**Hybrid Cloud Deployments**

Code42 provides customers with the choice of hybrid (or “mixed cloud”) deployments to enable customer choice in data storage location, including multi-destination storage. In some instances, sensitive data may require storage on-premises within destinations located in the customer data center only, while other data is cleared for public cloud storage. Alternatively, hybrid options are helpful when customer locations have varying levels of reliable Internet connectivity. Choice between public or private topology can be made site-by-site depending on the number of users, available bandwidth and latency. For example, an international location with many local users and poor Internet connectivity may be deployed as private cloud while the traveling sales team utilizes public cloud data storage.

Regardless of the deployment model selected (public, private or hybrid), Code42 offers consistency with security, reliability and performance.

**Conclusion**

Code42 protects data for customers within a range of security scenarios: from public cloud deployments for companies with employees located around the world, to private cloud deployments for government agencies held to the highest standard of information privacy.

From the ground up, Code42 products are built to address individual data security and compliance goals by giving customers explicit choice in features and functionality. In this way, Code42 supports its customers’ efforts to limit risk, meet regulatory requirements, and improve business resiliency and continuity.

Code42 has worked since 2001 to enable our customers to keep their data secure, choose how to meet their unique security and compliance obligations, and reduce the management burden on IT.

**INDEPENDENT VERIFICATIONS AND CERTIFICATIONS**

As a global service provider, Code42 is committed to continuous innovation to meet and exceed the standards and regulations for our industry and geographies. We’re currently certified for:

**PRIVATE/ON-PREMISES CLOUD DEPLOYMENTS\nSUPPORT YOUR DATA COMPLIANCE/GOVERNANCE EFFORTS**

Code42’s data protection solutions include features and functionality that—in concert with customer policies and procedures—support customer compliance efforts, such as:

- **HIPAA**
  Health Insurance Portability and Accountability Act

- **SOX**
  Sarbanes-Oxley Act

- **USFDA**
  U.S. Food and Drug Administration regulations

- **FISMA**
  Federal Information Security Management Act

- **PCI**
  Payment Card Industry

- **FERPA**
  Family Educational Rights and Privacy Act

- **GLBA**
  Gramm-Leach Bliley Act

- **USDOD**
  U.S. Department of Defense specifications

- **ITAR**
  International Traffic in Arms Regulations

**Business Associate Agreements**

Code42 can sign HIPAA Business Associate Agreements. A HIPAA Business Associate Agreement (BAA) is a contract between a HIPAA-Covered Entity and a HIPAA Business Associate (BA) that is used to protect electronic personal health information (ePHI) in accordance with HIPAA guidelines.