

## Reliable Data Protection HIPAA Compliance Summary

The Health Insurance Portability and Accountability Act (HIPAA) has several requirements as to the protection of Electronic Protected Health Information (EPHI). Reliable Data Protection enables firms to meet several of these requirements:

**DATA BACKUP PLAN (Required)** – A firm must have a data backup plan in place. By implementing Reliable Data Protection, they have implemented a data backup process and procedure. The information is moved offsite automatically for them on the schedule that they specify.

**DISASTER RECOVERY PLAN (Required)** – A firm must have a disaster recovery plan in place. While Reliable Data Protection does not provide a complete disaster recover plan for them (i.e. We do not help them find new office space), it does ensure that the data has been moved off-site in a secure fashion. Reliable Data Protection also ensures the data is held in a secure facility. Finally Reliable Data Protection enables them to restore their data once they are in their new facility.

**PHYSICAL ACCESS STANDARDS (Required)** – HIPAA requires that the covered entity “Implement Policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed”

Reliable Data Protection complies with this requirement in several ways. First, data backed up by Reliable Data Protection is encrypted at the source and the encryption key never leaves the source. Also, the data is transmitted over a secure communication channel (HTTP over SSL). Finally, the data is stored encrypted while in the data center. This ensures that no staff member of Reliable Data Protection has access to the data.

Beyond encryption, Reliable Data Protection also provides several key physical security features. The backed up data is stored within a Class A Data Center. This center has several physical security barriers. First, the floor of the building on which the Data Center is housed is accessible only by electronic card key. Second, The entrance to the data center is protected by a “Man Trap” that requires two electronic card key and pass code authorizations. Finally, the cage the equipment is housed in has a physical lock. If a thief were to get past all those barriers and get their hands on the data, they would find it useless as it was encrypted with an electronic key that is never transmitted to the data center.

**ENCRYPTION AND DECRYPTION (Required)** – HIPAA requires that the covered entity “Implement a mechanism to encrypt and decrypt electronic protected health information (EPHI)”.

Reliable Data Protection complies with this requirement as the data is encrypted the entire time it is within the Reliable Data Protection system. Decryption is performed only if the proper key is presented to the system.

**TRANSMISSION SECURITY (Required)** – HIPAA requires that the covered entity “Implement technical security measures to guard against unauthorized access to EPHI that is being transmitted over an electronic communications network”

Reliable Data Protection transmits the data that has already been encrypted over a secure HTTP over SSL connection, this is the same security measure that is used by banks to protect your financial information. HIPAA also requires that data modification be detectable. Reliable Data Protection provides for this by virtue of the base encryption process. If any data were modified, the decryption would fail, detecting the tampering.