Complion Disaster Recovery Overview

Complion Infrastructure

The Complion software platform is hosted in a Microsoft Azure cloud hosting provider. This data center is compliant with various regulatory legislation and has been third party-audited for controls and compliance.

Disaster Recovery Preparedness

Complion software hosting, deployment and release cycles are managed by experienced clinical research and IT professionals.

The following processes are performed to ensure continued management and support of the Complion application in preparation of a disaster recovery scenario:

- **Facility Security** – Data center hosting facility is staffed and monitored 24/7/365 with industry standard security, intrusion detection system, fire detection, uninterruptible power system, and alternate power generation equipment.
- **Backup Schedules** – The application and supporting databases are backed up and replicated to an offsite location in real-time to minimize the recovery point and allow the system to be restored at a particular point in time.
- **Audits** – Audits are performed with data center hosting providers.
- **Application Monitoring** – Proactive monitoring of the application and its infrastructure is performed by Complion.

Disaster Recovery Plan Overview

Complion has developed a comprehensive disaster recovery plan detailing the policies and procedures of Complion, Inc. in the event of a disruption to critical IT services. These processes ensure that those assets are recoverable to the right level and within the right timeframe to deliver a return to normal operations, with minimal impact on the business.

Disaster Recovery Plan details:

- Disaster Recovery Objectives
- Disaster Recovery Scope
- Testing Schedule
- Roles and Responsibilities
- Incident Response Plan
- DR Procedures

Key aspects of the DR plan include:

- Recovery Point Objective (RPO) is zero and achieved by real-time replication of data between Azure facilities;
- Recovery Time Objective (RTO) is 4 hours;
- Combination of automated failover and procedural failover components; and
- Client communication of any critical incident and failover occurrence.