Database Encryption (Optional)

As an option, Database Encryption, which will encrypt the database with AES-128 is offered for additional security.

DISASTER RECOVERY

Due to the nature of technology, unforeseen service outages may occur. In order to assure service reliability for hosted *ServicePoint* applications, WellSky offers the following disaster recovery options.

Basic Disaster Recovery Plan

The basic Disaster Recovery Plan is included in the standard *ServicePoint* contract and includes the following:

- Nightly database backups.
- Offsite storage of backups
- 7 day backup history stored locally on instantly accessible RAID storage
- 1 month backup history stored off site
- 24 x 7 access to WellSky's emergency line to provide assistance related to "outages" or "downtime".
- 24 hours backed up locally on instantly-accessible disk storage

Standard Recovery: All customer site databases are stored online, and are readily accessible for approximately 24 hours; backups are kept for approximately one (1) month. Upon recognition of a system failure, a site can be copied to a standby server, and a database can be restored, and site recreated within three (3) to four (4) hours if online backups are accessible. As a rule, a site restoration can be made within six (6) to eight (8) hours. On-site backups are made once daily and a restore of this backup may incur some data loss between when the backup was made and when the system failure occurred.

All internal servers are configured in hot-swappable hard drive RAID configurations. All systems are configured with hot-swappable redundant power supply units. Our Internet connectivity is comprised of a primary and secondary connection with separate internet service providers to ensure redundancy in the event of an ISP connectivity outage. The primary Core routers are configured with redundant power supplies, and are configured in tandem so that if one core router fails the secondary router will continue operation with little to no interruption in service. All servers, network devices, and related hardware are powered via APC Battery Backup units that in turn are all connected to electrical circuits that are connected to a building generator.

All client data is backed-up online and stored on a central file server repository for 24 hours. Each night an encrypted backup is made of these client databases and secured in an offsite datacenter.

Historical data can be restored from backups as long as the data requested is 30 days or newer. As a rule, the data can be restored to a standby server within 6-8 hours without affecting the current live site. Data can then be selectively queried and/or restored to the live site.

For power outage, our systems are backed up via APC battery back-up units, which are also in turn connected via generator-backed up electrical circuits. For a system crash, Non-Premium Disaster Recovery Customers can expect six (6) to eight (8) hours before a system restore with potential for some small data loss (data that was entered between the last backup and when the failure occurred) if a restore is necessary. If the failure is not hard drive related these times will possibly be much less since the drives themselves can be repopulated into a standby server.

All major outages are immediately brought to the attention of executive management. WellSky support staff helps manage communication or messaging to customers as progress is made to address the service outage. WellSky takes major outages seriously, understands, and appreciates that the customer becomes a tool and utility for daily activity and client service workflow.

Premium Disaster Recovery Plan (Optional)

The *optional* Premium Disaster Recovery plan includes all of the Basic Plan features plus several additional levels of support to enhance disaster recovery capability. Additional features included are as follows.

- Off site on a different Internet provider and on a separate electrical grid backups of the application server via a secured Virtual Private Network (VPN) connection
- Near-Instantaneous backups of application site (no files older than 15 minutes)
- Minute-level off site replication of database in case of a primary data center failure
- Priority level response (ensures downtime will not exceed 4 hours)

HIPAA COMPLIANCE

HIPAA compliance is a requirement for many organizations that use *ServicePoint,* particularly as the compliance relates to the HIPAA standards for security. The following methods ensure that *ServicePoint* is fully compliant with HIPAA data center standards.

- Network Security includes firewalls, certification servers, VPN access, and Operating System authentication.
- Encryption (optional – pricing is available upon request) is a database level security which encrypts confidential information located in the database tables.
- Audit Trails log and report on users who have viewed, updated, or deleted client records.
- Client Record Privacy Options allow or restrict access to all or part of a client file, including individual fields (data level).
- Automatic timeout logs a user out of the system after a specified period, thereby decreasing the potential viewing or manipulation of client data by unauthorized individuals.