SECURING CLIENT DATA

WellSky
11711 W. 79th St.
Lenexa, KS 66214
Phone: 1.855.WELLSKY
www.wellsky.com

WellSky
11711 W. 79th St., Lenexa, KS. 66214
WellSky.com | 1.855.WELLSKY

TABLE OF CONTENTS

SECURING CLIENT DATA

WellSky is committed to maintaining optimum client data security by meeting and exceeding industry standard practices. As a leader in software and Information Technology (IT) services for the health and human services industry, WellSky considers data security as the cornerstone of all of its development efforts. In 1999, WellSky pioneered its secured data-sharing model, enabling multi- agency collaboratives to collaborate while safeguarding client data (*ServicePoint* 1.0). In 2000, WellSky was the first web-based client data system to offer integrated database-level encryption. Again, in 2001, WellSky developed its integrated Audit Trail system before the HIPAA requirement.

WellSky has always held conviction that our products be fully web based and that we own and operate our own data center. We seek to provide best of class data center services to ensure data security and regulatory compliance, and continuously expand and invest in our data center to include physical security, network security, redundant power, redundant HVAC, fire suppression systems and full time staff to manage all of the afore mentioned.

This document outlines the measures taken by WellSky to secure all client data on each of our customers' *ServicePoint* site. The steps and precautions taken to ensure that data is stored and transmitted securely are divided into six main sections – Access Security, Site Security, Network Security, Disaster Recovery, HIPAA Compliance, and Unauthorized Access.

ACCESS SECURITY

Access Security begins at WellSky with a focus on the following areas:

- WellSky Employees
- WellSky Access to *ServicePoint*
- Audit Trails
- Customer Access to *ServicePoint*.

WellSky Employees

WellSky designated Security Officer assures employees are held to the highest standards when it comes to both company and customer data security. Employees who have access to client data are subject to a national background check, training on confidentiality requirements (company, HIPAA, HUD), and must sign a confidentiality statement as part of their employee agreement.

WellSky Access to ServicePoint

- Only a limited number of WellSky staff has access to a customer's *ServicePoint* site and client data. Access occurs only when you request an installation, import of data, implementation upgrade, or require assistance by support staff to troubleshoot a problem.

- The contract between the customer and WellSky legally compels WellSky to hold all client data stored in the customer's database in strict confidence. WellSky will take all reasonable precautions to prevent the disclosure to outside parties of such information, except as may be necessary by reason of legal, accounting or regulatory requirements.
- Access to the customer's system data by WellSky support staff can be monitored by running an *Audit Report* (see Automated Audit Trail below).

Audit Trail

- *ServicePoint* automatically tracks caller, client, and resource related activity by the use of an audit trail. This system function logs the time and type of activity, as well as the name of the user who viewed, added, edited, or deleted the information.
- All changes to Resource records are automatically tracked by the User (updates, as well as, date and time the updates were made). In addition, there is a Date of Official Update that is set when the Resource record has been formally reviewed. This section includes not only date and time of the Official update but also which User performed the action, which organization requested the Official Update, and a notes field for describing the reason for the update (such as Annual Review, Agency Request, etc.)
- To retrieve information created by the audit trail, an *Audit* report can be generated in the Reporting section of *ServicePoint*. Access to client audit information is limited to System Administrator and Agency Administrator access levels.

Customer Access to ServicePoint

- To ensure authorized access and to accommodate the auditing functions within the system, each user is issued a user name and password; both are required for entrance into the *ServicePoint* application.
  - Each *ServicePoint* user is required to have a unique User ID to log into the application.
  - Passwords must be 8 to 16 characters in length and must contain at least two numbers.
  - The system allows only one login per password at a time. A user cannot log into the system on two terminals at the same time using a single password.
  - Passwords automatically expire every 45 days requiring the user to create a new password.
    - A prompt appears when you need to choose a new password.
    - The same password cannot be used consecutively.
  - To enforce password security, *ServicePoint* will not allow a browser to save a password.
  - If FOUR consecutive logon attempts with the incorrect password are made, the user account will need to be reset by your System Administrator. This security feature prevents access to the site by a password generator.
  - Passwords are stored as hashed values in the *ServicePoint* database.

- *ServicePoint* has an automatic logout function for users who have been idle for a pre-determined period. (The default setting is 30 minutes.) This function decreases potential viewing and/or manipulation of client data by unauthorized individuals. Although the default setting is 30 minutes, each installation can request WellSky to set the system timeout for a length that meets their particular policies and procedures.
- To limit who can view and/or modify the customer's client data, individuals are assigned one of twenty (20) User Access Levels. Each user level has certain security restrictions applied to it. Each user level has access to certain *ServicePoint* features the ability to view certain pieces of client information. The System Administrators II role can see all data, even when it is closed.
  - Each level grants different access rights to the various sections (ClientPoint, ResourcePoint, SkanPoint, ShelterPoint, Admin etc.) of the application.

SITE SECURITY

Site security is a high priority since it not only protects the customer's stored client data, but also protects the equipment used to host the customer's data. To ensure the protection and service reliability for the customer's system, WellSky instituted the following security protocols:

Building Security

WellSky offices are located in a large commercial complex with the following perimeter security systems:

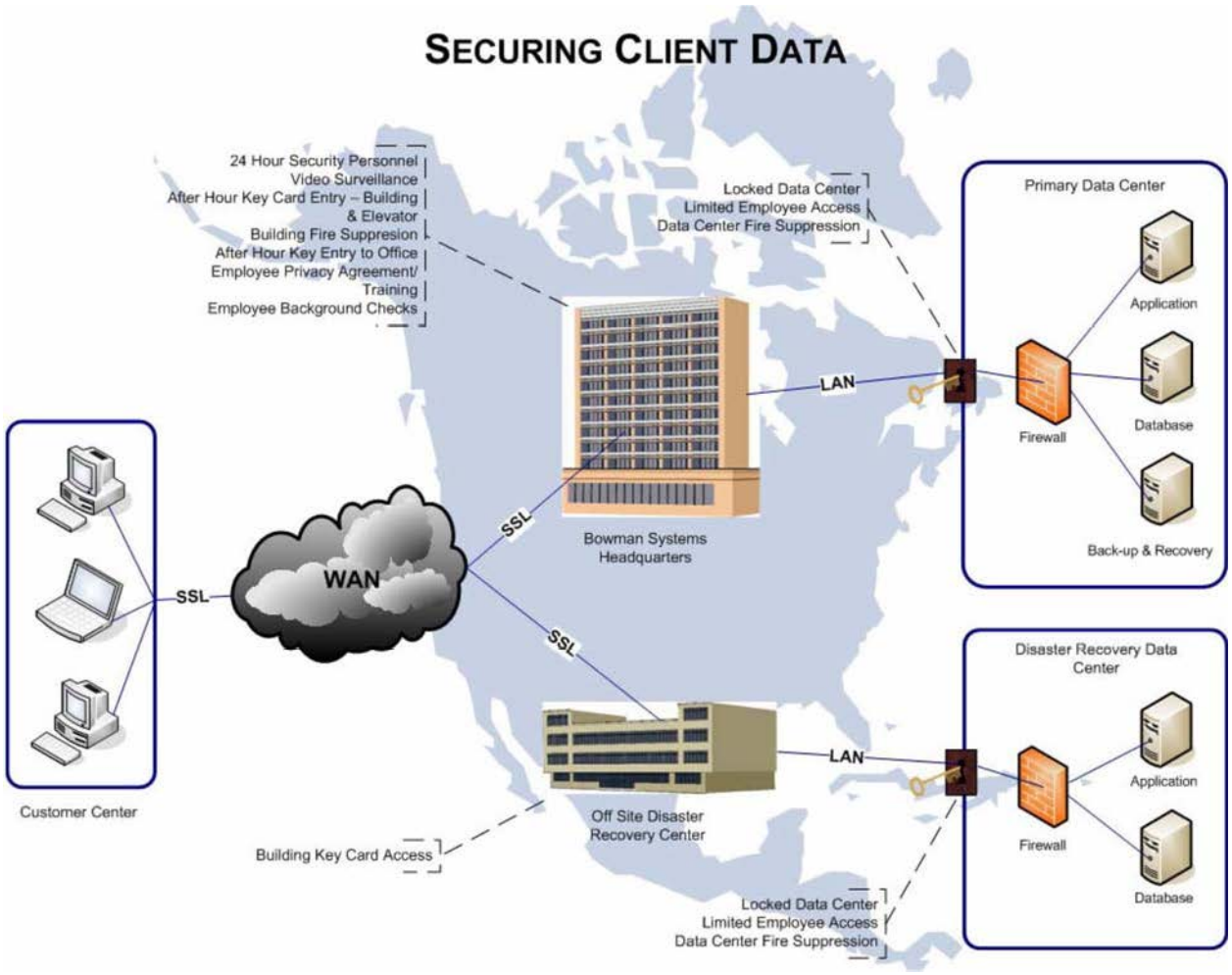
- 24-hour security personnel
- 24-hour video surveillance
- Building fire suppression system
- After-hours Key Card entry to building
- After-hours Key Card elevator access
- Locked stairwells during non-business hours.

WellSky Headquarters Security

The WellSky offices and data centers include the following additional levels of security.

- After-hours key entry to offices
- Dedicated and secured Data Center
  - Locked down 24-hours per day
  - Two separate, fully redundant HVAC systems for server areas

- Only accessible by management controlled key
- Protected by a state of the art, non-liquid automatic fire suppression system
- No access is permitted to the office cleaning staff
- Accessed by key personnel only (e.g. Information Technology and Management staff). Access is required for nightly data backups, new installations, upgrades and maintenance.



NETWORK SECURITY

Database security includes protection of client data residing on the database server and as it is transmitted over the internet through the application server. The security measures in place ensure that client data is only available to and accessed by authorized users.

There is a nightly backup of the *ServicePoint* system that is comprised of a backup of the database and a backup of the application code. Our standard protocol includes daily backup of the client's database to an off-site, out-of-state facility. WellSky maintains redundant power for all on-site servers via building power and building generator and redundant bandwidth provided via two separate upstream

providers. Our data center contains a state-of-the-art, non-destructive fire-suppression system. WellSky also utilizes RAID 10 (Redundant Array of Independent Disks) to mirror the hard drives, provide faster data throughput and ensure reliable data.

Other security measures are listed below.

- Multiple broadband connections, fully load balanced for reliability and speed.
- Reliable Enterprise class Cisco switches and routing equipment.
- A diesel powered generator capable of powering the facility indefinitely and UPS backups to supply uninterrupted power. This system is tested monthly (in such a way that power is not interrupted) to ensure reliability.
- Two separate, fully redundant HVAC systems for server areas.
- A non-liquid automatic fire control system.
- A physically secure building with keycard access, video surveillance and 24 x 7 security guard controlled access.

Data Security

To ensure availability of customer data in the event of system failure or malicious access, redundant records are created and stored in the following manner.

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

Firewalls

To enhance security further, firewalls are in place on all servers hosted by WellSky. As detailed below, there are multiple levels of firewall security.

- The *ServicePoint* application and database servers are separate from the WellSky's internal network.
- WellSky utilizes an industry standard Intrusion Detection System to pinpoint unauthorized attempts at accessing its network and to shield the customer's data in the event of such an attempt.
- Only regular and secured HTTP traffic are permitted through to the WellSky application servers.
- As a security policy, specifics on the type of equipment, protocols, and procedures in use are never revealed.
- Database servers are only accessible via an internal network connection from our application servers.

Encryption

SSL Encryption

SSL encryption ONLY encrypts the data going across the internet to the end-user's web browser. WellSky uses AES-256 encryption (Advanced Encryption Standard, 256-bit) in conjunction with RSA 2048-bit key lengths. A description can be found at http://en.wikipedia.org/wiki/Key_size.

When an end-user accesses their site, an SSL (encrypted) negotiation is performed between the server at WellSky's datacenter and the end user's web browser. The traffic that then flows between the server and the end user's workstation is encrypted using the SSL certificate installed on that server. This prevents anyone that is sitting in between our server here and the end user's workstation from being able to intercept potentially sensitive data. The AES-256 is the method in which the data is encrypted. There are various form

Public Key Infrastructure (PKI) (Optional)

As an option, Private Key Infrastructure (PKI) is available for those needing additional security frameworks. PKI is an additional layer of security on TOP of our standard SSL certificates. It is still SSL encrypted, however, this method of encryption requires a matching server certificate / client certificate pair in order to unencrypt the data that is sent from the end user's *ServicePoint* site to their Web Browser. Without the appropriate PKI client certificate installed on the end-user's workstation, their web browser will not be able to unencrypt the data and therefore will not be able to access the site. The PKI Client Certificate cannot be installed on a workstation without the appropriate password that accompanies the certificate. This allows the customer to regulate exactly who can and who cannot access their *ServicePoint* site.

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.

UNAUTHORIZED ACCESS

If an unauthorized entity were to gain access to a customer's system and client data or if there were suspicion of probable access, WellSky would take the following steps:

- The system would be examined to determine the presence of system or data corruption.
- If the system has been compromised, the system would be taken offline.
- Using the previous night's backup, a restored copy of the system data would be loaded onto another server, and the system brought back on line with the back-up data.
- Comparing the back-up database to the database taken offline, an investigation would be launched to determine the extent of the unauthorized activity/corruption, and the corrective action needed.
- Upon completion of the investigation, findings would be reported to the customer and options would be discussed.
- Upon customer approval, corrective action would be initiated. Corrective action could include all or part of the following:
  - The original hard drive would be completely erased and rebuilt, including a new operating system, SSL Certificate, application(s), and the back-up database.
  - If applicable and feasible, lost data from the original database would be restored.