REPORT ON

WELLSKY'S

DESCRIPTION OF ITS HEALTHCARE SOLUTIONS, AND ADVISORY AND OUTSOURCED SERVICES SYSTEMS AND ON THE SUITABILITY OF ITS CONTROLS RELEVANT TO SECURITY, AVAILABILITY, PROCESSING INTEGRITY, CONFIDENTIALITY, AND PRIVACY THROUGHOUT THE PERIOD

DECEMBER 1, 2021, TO NOVEMBER 30, 2022

MARCUM
ACCOUNTANTS ▲ ADVISORS

WellSky– SOC 3 TABLE OF CONTENTS

Acronym Table

AICPA	American Institute of Certified Public Accountants
ASA	Adaptive Security Appliance
AWS	Amazon Web Services
CPR	Cardiopulmonary Resuscitation
CRM	Customer Relationship Management
DDE	Direct Data Entry
FL	Florida
FNTS	First National Technology Solutions
GCP	Google Cloud Platform
HME	Home Medical Equipment
HR	Human Resources
IBM	International Business Machines
IDD	Intellectual or Developmental Disabilities
IP	Internet Protocol
IT	Information Technology
LTACH	Long Term Acute Care Hospital
LTSS	Long Term Services and Supports
NGINX	Engine X
OS	Operating System
PRTG	Paessler Router Traffic Grapher
RMM	Remote Monitoring Management
SaaS	Software as a Service
SFTP	Secure File Transfer Protocol
SIEM	Security Information and Event Management
SOC	System and Organization Controls
SQL	Structured Query Language
SUSE	Software Und System Entwicklung
TSC	Trust Service Criteria
TSP	Trust Service Principles
UPS	Uninterruptable Power Supply
VPN	Virtual Private Network
WellSky	WellSky Corporation
WSUS	Windows Server Update Services

Section 1: Assertion of the Management of WellSky

Assertion of the Management of WellSky

We are responsible for designing, implementing, operating, and maintaining effective controls within Healthcare Solutions and Advisory and Outsourced Services Systems throughout the period of December 1, 2021 to November 30, 2022, to provide reasonable assurance that WellSky's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (*With Revised Points of Focus- 2022)* in AICPA, *Trust Services Criteria*. Our description of the boundaries of the system is presented in Section 3 and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period December 1, 2021, to November 30, 2022, to provide reasonable assurance that WellSky's service commitments and system requirements were achieved based on applicable trust services criteria. WellSky's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Section 3.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of those inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period December 1, 2021 to November 30, 2022, to provide reasonable assurance that WellSky's service commitments and system requirements were achieved based on the applicable trust services criteria.

/s/ Steve Morgan, Chief Operating Officer
WellSky Corporation
January 30, 2023

Section 2: Independent Service Auditors' Report

MARCUM
ACCOUNTANTS ▲ ADVISORS

Independent Service Auditors' Report

To: WellSky

Scope

We have examined WellSky's accompanying assertion titled "Assertion of the Management of WellSky" (assertion) that the controls within Healthcare Solutions and Advisory and Outsourced Services Systemswere effective throughout the period December 1, 2021 to November 30, 2022, to provide reasonable assurance that WellSky's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (*With Revised Points of Focus- 2022)* in AICPA, *Trust Services Criteria*.

WellSky uses subservice organizations to provide cloud hosting, data center colocation services, as well as managed security monitoring for the production infrastructure. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at WellSky, to achieve WellSky's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

WellSky is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that WellSky's service commitments and system requirements were achieved. WellSky has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, WellSky is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditors' Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in

accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve WellSky's service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve WellSky's service commitments and system requirements based on the applicable trust services criteria.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Healthcare Solutions and Advisory and Outsourced Services Systems were effective throughout the period December 1, 2021 to November 30, 2022, to provide reasonable assurance that WellSky's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material aspects.

Marcum LLP

Marcum LLP

January 30, 2023
Tampa, FL

Section 3:WellSky's WellSky's Description of its Healthcare Solutions and Advisory Services Systems

Purpose and Scope of Report

This report on the internal controls placed in operation by WellSky is intended to provide interested parties with sufficient information to obtain an understanding of those aspects of WellSky's controls that may be relevant to a user entities' internal control structure. This report, when combined with an understanding of the policies and procedures at user entities, is intended to assist users in assessing controls of the user entities that may be affected by policies and procedures of WellSky's Healthcare Solutions and Advisory and Outsourced Services ("WellSky Solutions").

This report describes the system and control structure of WellSky as it relates to WellSky Solutions. It is intended to assist user entities in determining the adequacy of the internal controls that are outsourced to WellSky and are relevant to their internal control structures as it relates to security, availability, processing integrity, confidentiality, and privacy risks.

This description is intended to focus on the internal control structure of WellSky that is relevant to only users of WellSky Solutions and does not encompass all aspects of the services provided or procedures followed by WellSky.

System Description

Company Overview and Services Provided

WellSky is a technology company leading the movement for intelligent, coordinated care worldwide. WellSky is currently headquartered in Overland Park, Kansas, employing over 1500 employees in the United States. WellSky Solutions automate and streamline complex administrative processes as they relate to the health care industry. WellSky gives their clients the tools to improve efficiency and safety while measuring outcomes across functions, departments, and processes, while staying compliant. WellSky helps providers, payers, health systems, and community organizations solve tough challenges, improve collaboration for growth, harness the power of data analytics, and achieve better outcomes by further connecting clinical and social care.

WellSky offers the following software solutions and services:

- WellSky Transfusion – Stand-alone computer software intended to address all phases of blood transfusion services activities; may include the WellSky Transfusion Analytics feature, to monitor and measure key performance indicators for patient blood management, utilization, inventory, and blood bank operations.
- WellSky Biotherapies – Comprehensive clinical and laboratory management system that maximizes resources, scales production, and accelerates the understating of therapeutic potential and outcomes.
- WellSky Blood Centers – Comprehensive, modular, computerized system intended to be used by trained personnel as a tool in the management of data processes performed by staff at blood centers and high-volume blood testing services.

- WellSky Rehabilitation – Respiratory software utilized for determining staffing, managing protocols, respirator documentation and reporting tools.
- WellSky Specialty Care – A scalable and comprehensive health care information system built for long-term acute care hospitals. The solution is designed to help LTACHs improve clinical and financial function and leverage valuable insights across an organization.
- CareTend – Business management software utilized to streamline HME, home infusion, and specialty pharmacy operations.
- CPR+ – Business software suite that provides workflows, analytics and reporting, compliance, revenue management, inventory management, document management, patient care management, and data management to specialty pharmacies and home infusion providers.
- WellSky Home Health Therapy – Integrated point-of-care and back-office software solution for home health services.
- WellSky Hospice – Integrated comprehensive point-of-care and back-office hospice software solution.
- WellSky Consolo Hospice – Fully customizable, web-based hospice software suite that fosters compliance and clinical excellence.
- WellSky Palliative – Innovative palliative care software that empowers palliative providers to grow their programs and provide better care for patients.
- WellSky Personal Care – Customizable, web-based operating platform for personal care providers for optimizing care delivery.
- WellSky Medication Management – Pharmacy management software utilized at hospitals and pharmacies.
- WellSky Behavioral Health and IDD Provider – Behavioral health software utilized to streamline billing with complete revenue cycle management, track member demographics, provider performance, applications and contracts, service referrals and provision.
- WellSky Adult Day – Provides a software solution to enhance daily operations of adult day and care management businesses.
- WellSky Resource Manager – Healthcare capacity management software that enables the monitoring of patient demand, staff and resource utilization, and productivity to achieve organizational goals.
- CarePort – Comprehensive network management and Post-Acute Provider performance software suite, including Guide, Connect, Insight, Care Management, Transition, Referral Management, Discharge, and Intake.
- WellSky Human Services – Human Services SaaS solution built specifically for long-term services and support programs.
- WellSky Ombudsman – Human Services SaaS solution that provides intuitive and comprehensive case management that enables ombudsmen to track and manage nursing home complaint investigation from intake through closure more effectively.
- WellSky Aging and Disability – Care management system that supports the full delivery life cycle, from initial inquiry or referral to assessment, service delivery, and reporting.

- WellSky Community Services – Community information system that manages and coordinates services, guides resource allocation, and demonstrates effectiveness for multi-program agencies.
- WellSky Learning Center – Web based platform utilized to provide online education for hospice agencies.
- WellSky Revenue Cycle Services – Expert techniques to mitigate disruptions that impact reimbursement.
- WellSky DDE and Payer Connection – Provides a tool for home health and hospice agencies providing connection portals to Medicare and non-Medicare payers and claims processing tools.
- WellSky Social Care Coordination (formerly Healthify) - Empowers payers to identify social needs in a member population and coordinate care through a network of community-based partners to optimize quality of care, improve outcomes, lower costs, and increase member satisfaction.
- WellSky Home Care Coordination – Technology-enabled solution to contract, coordinate, refer, and schedule home-based care providers. Payers can curate scalable networks that support Medicare Advantage supplemental benefits offerings and Medicaid LTSS, and power alternative at-risk models of care in the home.
- WellSky Patient Engagement (formerly TapCloud) - Provides health care providers with patient metrics, and patients, or caregivers, with insights needed to confirm treatment progress, suggest alternative courses, or change medications.

Principal Service Commitments and System Requirements

WellSky designs its processes and procedures related to WellSky Solutions to meet its objectives. Those objectives are based on the service commitments that WellSky makes to user entities, the laws and regulations that govern SaaS providers, and the financial, operational, and compliance requirements that WellSky has established for the services.

Security commitments to user entities are documented in customer agreements. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of WellSky Solutions that are designed to permit system users to access the information they need based on the permission of least privilege provisioning.
- Use of encryption protocols to protect customer data at rest and in transit.

Availability commitments to user entities are documented in customer agreements. Availability commitments are standardized and include, but are not limited to, the following:

- Managing capacity demand through the monitoring and evaluation of current processing capacity and usage rates.
- Meeting Company objectives through authorization, design, development, and monitoring of data backup processes and recovery infrastructure.
- Environmental monitoring of conditions within key production areas.

Confidentiality commitments to user entities are documented in customer agreements. Confidentiality commitments are standardized and include, but are not limited to, the following:

- Information is defined and classified into categories with associated periods.
- Data retention and disposal policies and procedures are documented and in place.

Processing integrity commitments to user entities are documented in customer agreements. Processing integrity commitments are standardized and include, but are not limited to, the following:

- The company has defined data processing and reporting requirements, standards, and data sources.
- System inputs and outputs are measured and recorded completely, accurately, and timely.
- Policies and procedures are documented and in place to help ensure system processing results meet the entity's objectives.

Privacy commitments to user entities are documented in customer agreements. Privacy commitments are standardized and include, but are not limited to, the following:

- A privacy policy is documented and made available to all users including provisions for collection, use, disclosure, and disposal of personal information.

WellSky is a Service Provider. Privacy commitments are part of the services it provides to its clients and certain privacy commitments are not able to be designed, implemented, or effectively operated as they are applicable to data controllers. Services including interacting with the data subjects directly, obtaining consent of the end user in regard to their private information, and sharing information with third parties, are not in scope for a description of controls pertaining to the service commitments and system requirements of WellSky based on the applicable trust services criteria.

Therefore, it was determined that the following privacy criteria are not relevant to WellSky Solutions due to the following reasons:

- P2.1 –WellSky does not obtain explicit consent directly from data subjects; consent is the responsibility of the client as the Covered Entity.
- P3.2 – WellSky does not obtain explicit consent directly from data subjects; consent is the responsibility of the client as the Covered Entity.
- P5.1 – WellSky does not interact directly with data subjects as a data processor.
- P5.2 – WellSky does not interact directly with data subjects as a data processor.
- P6.1 –WellSky does not obtain explicit consent directly from data subjects; consent is the responsibility of the client as the Covered Entity.
- P6.7 – WellSky does not interact directly with data subjects as a data processor.
- P8.1 - WellSky does not interact directly with data subjects as a data processor.

WellSky establishes operational requirements that support the achievement of security, availability, processing integrity, confidentiality, and privacy commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in WellSky's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the WellSky Solutions.

Infrastructure

The infrastructure supporting WellSky Solutions include but is not limited to the following:

- Cisco ASA Firewall with FIREPOWER services
- Cisco AnyConnect VPN Gateway
- Palo Alto Networks Firewall and VPN Gateway
- Palo Alto GlobalProtect VPN Gateway
- Microsoft Windows Server
- Microsoft SQL Server
- MySQL production database
- Oracle production database
- PostgreSQL production database
- Linux servers including Amazon Linux, Ubuntu, SUSE and CentOS
- VMware Hypervisors
- Kubernetes and other containerization technologies
- F5, Citrix Netscaler and NGINX load balancers

The infrastructure for WellSky Solutions is segregated by application. Infrastructure for applications reside at secure offsite data centers and cloud hosting providers. The corporate network infrastructure at each location is used to facilitate secure access to the offsite data centers or to provide management of the corporate location assets.

Software

The following provides a summary of systems used to deliver WellSky's Healthcare Solutions and Advisory and Outsourced Services Systems:

- Accellion is a private cloud focused on secure file sharing used to deliver software solutions securely to customers.
- AWS S3 is utilized for storage of backups.
- Bitlocker is utilized as the hard disk encryption tool for Windows based OS machines. Citrix and GoGlobal are utilized for secure application delivery.

- Checkmarx and Vericode are used for Static Application Security Testing.
- Commvault is utilized as a backup tool for data center environments.
- Crowdstrike is used for antivirus protection for Company workstations and servers.
- ElasticSearch is used for search and analytics.
- FileVault is utilized as the hard disk encryption tool for MacOS based machines.
- IBM BigFix is utilized for patch management of Company servers.
- JAMF is used for centralized managed of Apple devices.
- JIRA is utilized as an IT ticketing system to document issues and resolutions.
- WellSky Academy with content from Biz Library is used as an internal training and documentation tool for WellSky's employees.
- Microsoft M365 is used for email, collaboration and web conferencing.
- Nagios is utilized for uptime and availability monitoring of Company systems.
- New Relic is utilized as the application-monitoring tool within the AWS environment.
- Okta is utilized for multi-factor authentication and Single Sign-on.
- Pager Duty is utilized for system monitoring notifications.
- PRTG is utilized to analyze network events, block traffic and report possible breach attempts.
- PulseWay is utilized as the RMM tool for monitoring data center environments.
- Salesforce is utilized as the CRM for managing and storing customer data.
- SecureLink is utilized for secure, audited access to sensitive systems.
- Sisense is used for data analytics and warehousing.
- Site 24x7 is utilized as the application monitoring tool for the production application.
- Snyk is utilized for open source library vulnerabilities.
- Splunk is utilized as the SIEM tool for system logging within the data center environments.
- Sumologic is utilized for operational logging.
- Veeam is utilized as the backup technology for the data center environments.
- WSUS is utilized for patch management of Company servers.
- Zabbix is utilized for uptime and availability monitoring of Company systems.
- Zoom is used for web conferencing and telephone services.

People

The following provides a summary of people involved in the operation and use of WellSky Solutions:

- Chief Technology Officer – Who is responsible for lead design and development.
- Senior Director, Corporate IT – Who is responsible for oversight of the Corporate IT department.
- Vice President, Information Security – Who is responsible for security and availability of the WellSky Solutions.
- Director, Infrastructure Operations – Who is responsible for product research and development.

- Senior Vice President, Compliance – Who serves as the Compliance Officer and is responsible for implementation and management of WellSky's Compliance Program.
- Sr. Regulatory Compliance Manager – Who is responsible for security awareness and overall compliance.

Procedures

The following provides a summary of policies maintained and documented by Executive and Operations Management personnel involved in the operation of WellSky Solutions:

- Access Control
- Awareness and Training
- Audit and Accountability
- Backup
- Configuration Management
- Contingency Planning
- Data Classification and Handling
- Identification and Authentication
- Information Security Practices Policy
- Incident Response
- Maintenance
- Media Protection
- Physical and Environmental Protection Planning
- Personnel Security
- Privacy Compliance Evaluation and Auditing
- Risk Assessment
- Security Assessment and Authorization
- System and Communications Protection
- System and Information Integrity
- System and Services Acquisition
- System Security Plan

Control activities have been placed into operation to help ensure that actions are conducted properly and efficiently. Control procedures serve as mechanisms for managing the achievement of control activities and are a part of the process by which WellSky strives to achieve its business objectives. WellSky has applied a risk management approach to the organization in order to select and develop control procedures. After relevant risks have been identified and evaluated, controls are established, implemented, monitored, reviewed, and improved, when necessary, to meet the applicable trust services criteria and the overall objectives of the organization.

The WellSky control procedures, which have been designed to meet the applicable trust services criteria, are included in Section 4 of this report to eliminate the redundancy that would result from listing the procedures in this section as well.

Data

WellSky Solutions include customizable services and reports to meet the specialized needs of clients as well as automated order and delivery options via the web or secure e-mail. WellSky receives customer information via mail, secure e-mail, SFTP, and WellSky's SaaS systems. Electronic data is protected via logical access controls, encryption, and network protection devices.

Printed documents are handled and stored in secured locations and items requiring disposal are shredded appropriately.

System Boundaries

System boundaries, pertaining to collection, use, retention, disclosure, and disposal or anonymization or personalization of data, are governed by contract provisions for particular service engagements. Data is not utilized or disclosed to third parties outside of the scope allowed in such contracts and agreements.

Significant Changes to the System Throughout the Period

There were no significant changes throughout the period.

Subservice Organizations

The company uses subservice organizations to perform certain functions to improve operating and administrative effectiveness. All subservice organizations listed below provide annual attestation reports to WellSky as part of the vendor management program. WellSky monitors the security, availability, processing integrity, confidentiality, and privacy commitments and obtains attestation reports and/or other supporting documentation, when applicable, on an annual basis to help ensure that security, availability, processing integrity, confidentiality, and privacy commitments are being met and reflect the current security environment.

The accompanying description includes only relevant policies, procedures, and Trust Service Criteria and activities of the company and does not include policies, procedures, or Trust Services Criteria and activities of the third-party service organizations described below. The following subservice organizations are used by WellSky for the following:

Service Providers	Nature of Service Provided
TierPoint	Data center colocation
Zayo	Data center colocation
FNTS	Managed data center services
Connectria	Managed data center services
Data Foundry	Data center colocation
AWS	Cloud Hosting

Service Providers	Nature of Service Provided
Iron Mountain	Data center colocation
Flexential (Formerly Peak 10)	Data center colocation
Azure	Cloud Hosting
Google Cloud Platform	Cloud Hosting
Prominic	Managed Date Center Services
Kudelski	Managed security services
Aptible	Platform as a Service
Black Hills Information Security	Penetration Testing and Training

TierPoint

WellSky uses TierPoint for their data center services. TierPoint is responsible for the uptime and management of the IP transit services, physical security, and environmental conditions that provide power and cooling to their devices.

The applicable trust services criteria that are intended to be met by controls at TierPoint, alone or in combination with controls at WellSky, and the types of controls expected to be implemented at TierPoint to meet those criteria are described in the tables below:

Control Activities Expected to be Implemented by TierPoint	Applicable Trust Services Criteria
TierPoint is responsible for restricting physical access to and within the data center facilities.	CC6.4
TierPoint is responsible for implementing measures to prevent or mitigate threats consistent with the risk assessment.	CC3.1, CC3.2, CC7.1
TierPoint is responsible for monitoring environmental conditions (temperature, fire, and water), leak detection, UPS battery life and capacity, and other key equipment to help maintain availability of services.	A1.1, A1.2
TierPoint is responsible for maintaining availability of internet and power services, as well as preventative maintenance of cooling and power equipment.	A1.2
TierPoint is responsible for performing load testing on generators and UPS devices, as well as annual disaster recovery testing.	A1.2

Zayo

WellSky uses Zayo for their data center services. Zayo is responsible for the uptime and management of the IP transit services, physical security, and environmental conditions that provide power and cooling to their devices.

The applicable trust services criteria that are intended to be met by controls at Zayo, alone or in combination with controls at WellSky, and the types of controls expected to be implemented at Zayo to meet those criteria are described in the tables below:

Control Activities Expected to be Implemented by Zayo	Applicable Trust Services Criteria
Zayo is responsible for restricting physical access to and within the data center facilities.	CC6.4
Zayo is responsible for implementing measures to prevent or mitigate threats consistent with the risk assessment.	CC3.1, CC3.2, CC7.1
Zayo is responsible for monitoring environmental conditions (temperature, fire, and water), leak detection, UPS battery life and capacity, and other key equipment to help maintain availability of services.	A1.1, A1.2
Zayo is responsible for maintaining availability of internet and power services, as well as preventative maintenance of cooling and power equipment.	A1.2
Zayo is responsible for performing load testing on generators and UPS devices, as well as annual disaster recovery testing.	A1.2

FNTS

WellSky uses FNTS for their managed IT hosting services. FNTS is responsible for the uptime and management of the IP transit services, physical security, and environmental conditions that provide power and cooling to their devices. FNTS is also responsible for properly implementing changes requested by the authorized WellSky individuals as part of the services provided.

The applicable trust services criteria that are intended to be met by controls at FNTS, alone or in combination with controls at WellSky, and the types of controls expected to be implemented at FNTS to meet those criteria are described in the table below:

Control Activities Expected to be Implemented by FNTS	Applicable Trust Services Criteria
FNTS is responsible for restricting logical and physical access to and within the data center facilities and system components including firewalls, routers, and servers, and facility management software.	CC6.1, CC6.2, CC6.3, CC6.4,

Control Activities Expected to be Implemented by FNTS	Applicable Trust Services Criteria
FNTS is responsible for implementing measures to prevent or mitigate threats consistent with the risk assessment.	CC3.1, CC3.2, CC7.1
FNTS is responsible for notifying WellSky of any suspected or actual security incidents and containing, remediating and communicating security incidents as appropriate.	CC7.3, CC7.4
FNTS is responsible for monitoring environmental conditions (temperature, fire, and water), leak detection, UPS battery life and capacity, and other key equipment to help maintain availability of services.	A1.1, A1.2
FNTS is responsible for maintaining availability of internet and power services, as well as preventative maintenance of cooling and power equipment.	A1.2
FNTS is responsible for monitoring hosted IT systems availability to help maintain availability of services.	A1.2
FNTS is responsible for performing load testing on generators and UPS devices, as well as annual disaster recovery testing.	A1.3
FNTS is responsible for the management of any third-party vendors with access to customer environments.	CC9.2, C1.1, C1.2

Connectria

WellSky uses Connectria for their managed IT hosting services. Connectria is responsible for the uptime and management of the IP transit services, physical security, and environmental conditions that provide power and cooling to their devices. Connectria is also responsible for properly implementing changes requested by the authorized WellSky individuals as part of the services provided.

The applicable trust services criteria that are intended to be met by controls at Connectria, alone or in combination with controls at WellSky, and the types of controls expected to be implemented at Connectria to meet those criteria are described in the table below:

Control Activities Expected to be Implemented by Connectria	Applicable Trust Services Criteria
Connectria is responsible for restricting logical and physical access to and within the data center facilities and system components including firewalls, routers, and servers, and facility management software.	CC6.1, CC6.2, CC6.3, CC6.4
Connectria is responsible for implementing measures to prevent or mitigate threats consistent with the risk assessment.	CC3.1, CC3.2, CC7.1

Control Activities Expected to be Implemented by Connectria	Applicable Trust Services Criteria
Connectria is responsible for notifying WellSky of any suspected or actual security incidents and containing, remediating and communicating security incidents as appropriate.	CC7.3, CC7.4
Connectria is responsible for monitoring environmental conditions (temperature, fire, and water), leak detection, UPS battery life and capacity, and other key equipment to help maintain availability of services.	A1.1, A1.2
Connectria is responsible for maintaining availability of internet and power services, as well as preventative maintenance of cooling and power equipment.	A1.2
Connectria is responsible for monitoring hosted IT systems availability to help maintain availability of services.	A1.2
Connectria is responsible for performing load testing on generators and UPS devices, as well as annual disaster recovery testing.	A1.3
Connectria is responsible for the management of any third-party vendors with access to customer environments.	CC92, C1.1, C1.2

Data Foundry

WellSky uses Data Foundry for their data center services. Data Foundry is responsible for the uptime and management of the IP transit services, physical security, and environmental conditions that provide power and cooling to their devices.

The applicable trust services criteria that are intended to be met by controls at Data Foundry, alone or in combination with controls at WellSky, and the types of controls expected to be implemented at Data Foundry to meet those criteria are described in the tables below:

Control Activities Expected to be Implemented by Data Foundry	Applicable Trust Services Criteria
Data Foundry is responsible for restricting physical access to and within the data center facilities.	CC6.4
Data Foundry is responsible for implementing measures to prevent or mitigate threats consistent with the risk assessment.	CC3.1, CC3.2, CC7.1
Data Foundry is responsible for monitoring environmental conditions (temperature, fire, and water), leak detection, UPS battery life and capacity, and other key equipment to help maintain availability of services.	A1.2

Control Activities Expected to be Implemented by Data Foundry	Applicable Trust Services Criteria
Data Foundry is responsible for maintaining availability of internet and power services, as well as preventative maintenance of cooling and power equipment.	A1.2
Data Foundry is responsible for performing load testing on generators and UPS devices, as well as annual disaster recovery testing.	A1.2
Data Foundry is responsible for restricting physical access to and within the data center facilities.	CC6.4

AWS

AWS is utilized for production system hosting. AWS is responsible for the uptime, management, and physical security of their infrastructure that supports the delivery the production hosting services and environmental conditions that provide power and cooling to their devices. AWS is responsible for providing physical security controls, administration of their hardware equipment, and reporting any logical or physical security incidents.

The applicable trust services criteria that are intended to be met by controls at AWS, alone or in combination with controls at WellSky, and the types of controls expected to be implemented at AWS to meet those criteria are described in the tables below:

Control Activities Expected to be Implemented by AWS	Applicable Trust Services Criteria
AWS is responsible for restricting logical and physical access to and within the data center facilities and system components including firewalls, routers, and servers, and facility management software.	CC6.2, CC6.3, CC6.4, CC6.6, CC6.7
AWS is responsible for implementing measures to prevent or mitigate threats consistent with the risk assessment.	CC3.1, CC3.2, CC7.1
AWS is responsible for monitoring environmental conditions (temperature, fire, and water), leak detection, UPS battery life and capacity, and other key equipment to help maintain availability of services.	A1.2
AWS is responsible for maintaining availability of internet and power services, as well as preventative maintenance of cooling and power equipment.	A1.2
AWS is responsible for maintaining logical segregation of virtualized environments from other AWS clients.	CC6.1, CC6.2

Iron Mountain

WellSky uses Iron Mountain for their data center services. Iron Mountain is responsible for the uptime and management of the IP transit services, physical security, and environmental conditions that provide power and cooling to their devices.

The applicable trust services criteria that are intended to be met by controls at Iron Mountain, alone or in combination with controls at WellSky, and the types of controls expected to be implemented at Iron Mountain to meet those criteria are described in the tables below:

Control Activities Expected to be Implemented by Iron Mountain	Applicable Trust Services Criteria
Iron Mountain is responsible for restricting physical access to and within the data center facilities.	CC6.4
Iron Mountain is responsible for implementing measures to prevent or mitigate threats consistent with the risk assessment.	CC3.1, CC3.2, CC7.1
Iron Mountain is responsible for monitoring environmental conditions (temperature, fire, and water), leak detection, UPS battery life and capacity, and other key equipment to help maintain availability of services.	A1.2
Iron Mountain is responsible for maintaining availability of internet and power services, as well as preventative maintenance of cooling and power equipment.	A1.2
Iron Mountain is responsible for performing load testing on generators and UPS devices, as well as annual disaster recovery testing.	A1.2
Iron Mountain is responsible for restricting physical access to and within the data center facilities.	CC6.4

Flexential (Peak 10)

WellSky uses Flexential for their data center services. Flexential is responsible for the uptime and management of the IP transit services, physical security, and environmental conditions that provide power and cooling to their devices.

The applicable trust services criteria that are intended to be met by controls at Flexential, alone or in combination with controls at WellSky, and the types of controls expected to be implemented at Flexential to meet those criteria are described in the tables below:

Control Activities Expected to be Implemented by Flexential	Applicable Trust Services Criteria
Flexential is responsible for restricting physical access to and within the data center facilities.	CC6.4

Control Activities Expected to be Implemented by Flexential	Applicable Trust Services Criteria
Flexential is responsible for implementing measures to prevent or mitigate threats consistent with the risk assessment.	CC3.1, CC3.2, CC7.1
Flexential is responsible for monitoring environmental conditions (temperature, fire, and water), leak detection, UPS battery life and capacity, and other key equipment to help maintain availability of services.	A1.2
Flexential is responsible for maintaining availability of internet and power services, as well as preventative maintenance of cooling and power equipment.	A1.2
Flexential is responsible for performing load testing on generators and UPS devices, as well as annual disaster recovery testing.	A1.2
Flexential is responsible for restricting physical access to and within the data center facilities.	CC6.4

Azure

Azure is utilized for production system hosting. Azure is responsible for the uptime, management, and physical security of their infrastructure that supports the delivery the production hosting services and environmental conditions that provide power and cooling to their devices. Azure is responsible for providing physical security controls, administration of their hardware equipment, and reporting any logical or physical security incidents.

The applicable trust services criteria that are intended to be met by controls at Azure, alone or in combination with controls at WellSky, and the types of controls expected to be implemented at Azure to meet those criteria are described in the tables below:

Control Activities Expected to be Implemented by Azure	Applicable Trust Services Criteria
Azure is responsible for restricting logical and physical access to and within the data center facilities and system components including firewalls, routers, and servers, and facility management software.	CC6.2, CC6.3, CC6.4, CC6.6, CC6.7
Azure is responsible for implementing measures to prevent or mitigate threats consistent with the risk assessment.	CC3.1, CC3.2, CC7.1
Azure is responsible for monitoring environmental conditions (temperature, fire, and water), leak detection, UPS battery life and capacity, and other key equipment to help maintain availability of services.	A1.2
Azure is responsible for maintaining availability of internet and power services, as well as preventative maintenance of cooling and power equipment.	A1.2
Azure is responsible for maintaining logical segregation of virtualized environments from other Azure clients.	CC6.1, CC6.2

Google Cloud Platform (GCP)

GCP is utilized for production system hosting. GCP is responsible for the uptime, management, and physical security of their infrastructure that supports the delivery the production hosting services and environmental conditions that provide power and cooling to their devices. GCP is responsible for providing physical security controls, administration of their hardware equipment, and reporting any logical or physical security incidents.

The applicable trust services criteria that are intended to be met by controls at GCP, alone or in combination with controls at WellSky, and the types of controls expected to be implemented at GCP to meet those criteria are described in the tables below:

Control Activities Expected to be Implemented by GCP	Applicable Trust Services Criteria
GCP is responsible for restricting logical and physical access to and within the data center facilities and system components including firewalls, routers, and servers, and facility management software.	CC6.2, CC6.3, CC6.4, CC6.6, CC6.7
GCP is responsible for implementing measures to prevent or mitigate threats consistent with the risk assessment.	CC3.1, CC3.2, CC7.1
GCP is responsible for monitoring environmental conditions (temperature, fire, and water), leak detection, UPS battery life and capacity, and other key equipment to help maintain availability of services.	A1.2
GCP is responsible for maintaining availability of internet and power services, as well as preventative maintenance of cooling and power equipment.	A1.2
GCP is responsible for maintaining logical segregation of virtualized environments from other GCP clients.	CC6.1, CC6.2

Prominic

WellSky uses Prominic for their data center services. Prominic is responsible for the uptime and management of the IP transit services, physical security, and environmental conditions that provide power and cooling to their devices.

The applicable trust services criteria that are intended to be met by controls at Prominic, alone or in combination with controls at WellSky, and the types of controls expected to be implemented at Prominic to meet those criteria are described in the tables below:

Control Activities Expected to be Implemented by Prominic	Applicable Trust Services Criteria
Prominic is responsible for restricting physical access to and within the data center facilities.	CC6.4

Control Activities Expected to be Implemented by Prominic	Applicable Trust Services Criteria
Prominic is responsible for maintaining logical segregation of virtualized environments from other Prominic clients.	CC6.1, CC6.2
Prominic is responsible for implementing measures to prevent or mitigate threats consistent with the risk assessment.	CC3.1, CC3.2, CC7.1
Prominic is responsible for monitoring environmental conditions (temperature, fire, and water), leak detection, UPS battery life and capacity, and other key equipment to help maintain availability of services.	A1.2
Prominic is responsible for maintaining availability of internet and power services, as well as preventative maintenance of cooling and power equipment.	A1.2
Prominic is responsible for performing load testing on generators and UPS devices, as well as annual disaster recovery testing.	A1.2
Prominic is responsible for restricting physical access to and within the data center facilities.	CC6.4

Kudelski

WellSky uses Kudelski for managed security services. Kudelski is responsible for the analysis of security logs and reporting any potential security alerts to WellSky management.

The applicable trust services criteria that are intended to be met by controls at Kudelski, alone or in combination with controls at WellSky, and the types of controls expected to be implemented at Kudelski to meet those criteria are described in the tables below:

Control Activities Expected to be Implemented by Kudelski	Applicable Trust Services Criteria
Kudelski is responsible for reporting security incidents detected via system monitoring tools to WellSky management.	CC7.3

Aptible

Aptible is utilized for their platform as a service. Aptible is responsible for the uptime, management, and physical security of their infrastructure that supports the delivery the production hosting services and environmental conditions that provide power and cooling to their devices. Aptible is responsible for providing physical security controls, administration of their hardware equipment, and reporting any logical or physical security incidents.

The applicable trust services criteria that are intended to be met by controls at Aptible, alone or in combination with controls at WellSky, and the types of controls expected to be implemented at Aptible to meet those criteria are described in the tables below:

Control Activities Expected to be Implemented by Aptible	Applicable Trust Services Criteria
Aptible is responsible for restricting logical and physical access to and within the data center facilities and system components including firewalls, routers, and servers, and facility management software.	CC6.2, CC6.3, CC6.4, CC6.6, CC6.7
Aptible is responsible for implementing measures to prevent or mitigate threats consistent with the risk assessment.	CC3.1, CC3.2, CC7.1
Aptible is responsible for monitoring environmental conditions (temperature, fire, and water), leak detection, UPS battery life and capacity, and other key equipment to help maintain availability of services.	A1.2
Aptible is responsible for maintaining availability of internet and power services, as well as preventative maintenance of cooling and power equipment.	A1.2
Aptible is responsible for maintaining logical segregation of virtualized environments from other Aptible clients.	CC6.1, CC6.2

Black Hills Information Security

WellSky uses Black Hills Information Security for penetration testing services. Black Hills Information Security is responsible for the analysis of penetration testing results and reporting to WellSky management.

The applicable trust services criteria that are intended to be met by controls at Black Hills Information Security, alone or in combination with controls at WellSky, and the types of controls expected to be implemented at Black Hills Information Security to meet those criteria are described in the tables below:

Control Activities Expected to be Implemented by Black Hills Information Security	Applicable Trust Services Criteria
Black Hills Information Security is responsible for reporting security incidents detected via system monitoring tools to WellSky management.	CC7.3

On an annual basis WellSky obtains a third party SOC 2 Type II report from the subservice organizations and reviews the report and testing results to determine if there were appropriate controls and that they were operating effectively. In the event there are exceptions or controls not operating effectively at a subservice organization this risk is incorporated into a risk assessment and appropriate actions are taken to mitigate risks in the future.

Control Environment

The control environment is determined by the control consciousness of an organization, which sets the tone of an organization, and the way personnel conduct their activities, influencing how they carry out their control functions. This is the foundation for all other components of internal control, providing discipline and structure for business operations.

The control environment at WellSky begins with management's philosophy and operating style as well as the priorities and direction provided by the Executive Management team. WellSky's entire organization is dedicated to delivering the highest level of customer service. The company has created a corporate culture that supports this mission.

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of the control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the products of the entity's ethical and behavioral standards, how they are communicated and how they are reinforced in practice. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements, codes of conduct, and leadership example.

WellSky has implemented, maintains, and regularly communicates a code of conduct and other policies regarding acceptable business practices, guidance on conflicts of interest, and expected standards of ethical and moral behavior. WellSky's management conducts business dealings with employees, suppliers, customers, investors, creditors, competitors, agents, resellers, counsel, accountants, and auditors on a high ethical plane and insists others have similar business practices.

Commitment to Competence

Competence is the knowledge and skills necessary to accomplish tasks that define the individual's job. Commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into requisite skills and knowledge.

WellSky assigns job responsibilities to personnel based on knowledge and skills needed to adequately perform each job. WellSky reinforces these responsibilities by providing hands-on training during the initial period of employment, and continual hands-on training for new business processes or job responsibilities.

Management's Philosophy and Operating Style

Management's philosophy and operating style encompass a broad range of characteristics. Such characteristics may include the following: management's approach to taking and monitoring business risk; management's attitude and actions for the security and confidentiality of information. WellSky's management takes a relatively conservative approach to information processing and risk associated with new business ventures.

Organizational Structure

An entity's organizational structure provides the framework for how entity-wide objectives are

planned, executed, controlled, and monitored. A relevant organizational structure includes considering key areas of authority and responsibility and appropriate lines of reporting. An entity develops an organizational structure contingent, in part, on its size and the nature of its activities.

The responsibilities of key positions within WellSky are clearly defined and communicated to personnel. Individuals that hold key positions are knowledgeable and experienced within the industry. WellSky's organizational structure supports communication of information both up to leadership as well as down to support staff. WellSky's organizational structure is comprised of six primary business units that work together to deliver WellSky Solutions.

The seven business units consist of:

- Executive Management – Responsible for providing execution of business objectives and strategic direction.
- Engineering – Responsible for creating new functionality, maintaining existing code, overseeing security, and managing physical systems. They are also involved with the implementation of systems, tests of system software releases, daily monitoring of system performance, and resolution of software bugs. The Engineering team delivers software, manages security administration, and maintains policies and procedures manuals for the processing environment.
- IT – Responsible for designing, implementing, and managing IT infrastructure and operations.
- Compliance – Responsible for auditing and regulatory compliance.
- Finance and Administration – Coordinates WellSky's services and operations, including service billing.
- People & Talent – Manages the human resources (HR) function for WellSky. Conducts background and security checks on WellSky teammates prior to employment, and provides a mandatory orientation program to teammates. The confidentiality of client and facility information is stressed during the new hire orientation program and is also addressed in the policies and procedures issued to each teammate at time of hire. New teammates are given the necessary job training to meet the expectations of their position including security, confidentiality, privacy, and compliance requirements.
- Sales and Marketing – Provides analysis for new business prospects and new service offerings. Supports the company market position and brand/image management through a variety of marketing tactics. Develops and manages client relationships.

Assignment of Authority and Responsibility

Assignment of authority and responsibility includes delegation of authority to deal with organizational goals and objectives, operating functions and regulatory requirements, including responsibility for information systems and authorizations for changes. Policies are established relating to business practices, knowledge and experience required of key personnel, and the appropriate number of people to carry out duties. In addition, management's policies and communications are directed at ensuring that personnel understand the entity's objectives, know

how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

WellSky has defined job responsibilities and clear communication channels to disseminate information within the organization; this enables WellSky to react to market and regulation changes and to meet its goals and objectives. WellSky is appropriately staffed to support its operations, particularly with respect to critical areas such as software development, implementation, customer support, and information technology system support.

Human Resource Policies and Practices

HR policies and practices relate to hiring, orientation, training, evaluating, counseling, and Corrective action. Standards for hiring the most qualified individuals with emphasis on prior work experience, past accomplishments, educational background, , and evidence of integrity and ethical behavior demonstrate WellSky's commitment to hiring and retaining only highly competent and trustworthy people. Career growth and development are driven by periodic performance feedback and demonstrate WellSky's commitment to advance qualified individuals to higher levels of responsibility. Personnel employed by WellSky are required to read and acknowledge the WellSky's internal policies and confidentiality requirements as well as the confidentiality of client managed information at the time of hire and on an annual basis.

Risk Assessment

WellSky's management performs periodic risk assessments, which requires management to identify risks in its areas of responsibility and to implement appropriate measures to address those risks. WellSky's management reevaluates the risk assessment at least annually to both update the previous results and to identify any new potential areas of concern.

The risk assessment process consists of the following phases:

- Identifying – The identification phase includes listing out risks (including threats and vulnerabilities) that exist in the environment. This phase provides a basis for all other risk management activities.
- Assessing – The assessment phase considers the potential impact(s) of identified risks to the service organization and their likelihood of occurrence.
- Mitigating – The mitigation phase includes putting controls, processes, and other physical and virtual safeguards in place to prevent and detect both identified and assessed risks.
- Reporting – The reporting phase results in risk reports provided to managers with the necessary data to make effective business decisions and to comply with internal policies and any applicable regulations.
- Monitoring – The monitoring phase includes the performance of monitoring activities by WellSky's management team to evaluate whether the processes, initiatives, functions or activities are mitigating the risk as designed.

In-Scope Trust Service Categories

The table below provides the TSC within the scope of this report. The controls designed and implemented to meet the applicable TSC criteria have been included in Section 4.

Trust Services Categories	Definition
Security	Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to meet its objectives.
Availability	Information and systems are available for operation and use to meet the entity's commitments.
Processing Integrity	System processing is complete, valid, accurate, timely, and authorized to meet the entity's commitments and system requirements.
Confidentiality	Information designated as confidential is protected to meet the entity's commitments and system requirements.
Privacy	Personal information is collected, used, retained, disclosed, and disposed to meet the entity's commitments and system requirements.

Security

Security refers to the protection of:

- Information during its collection or creation, use, processing, transmission, and storage and
- Systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

Availability

Availability refers to the accessibility of information used by the entity's systems, as well as the products or services provided to its customers. The availability objective does not, in itself, set a minimum acceptable performance level; it does not address system functionality (the specific functions a system performs) or usability (the ability of users to apply system functions to the performance of specific tasks or problems). However, it does address whether systems include controls to support accessibility for operation, monitoring, and maintenance.

Processing Integrity

Processing integrity refers to the completeness, validity, accuracy, timeliness, and authorization of system processing. Processing integrity addresses whether systems achieve the aim or purpose for which they exist and whether they perform their intended functions in an unimpaired manner, free from error, delay, omission, and unauthorized or inadvertent manipulation. Because of the number

of systems used by an entity, processing integrity is usually only addressed at the system or functional level of an entity.

Confidentiality

Confidentiality addresses the entity's ability to protect information designated as confidential from its collection or creation through its final disposition and removal from the entity's control in accordance with management's objectives. Information is confidential if the custodian (for example, an entity that holds or stores information) of the information is required to limit its access, use, and retention and restrict its disclosure to defined parties (including those who may otherwise have authorized access within its system boundaries). Confidentiality requirements may be contained in laws or regulations or in contracts or agreements that contain commitments made to customers or others. The need for information to be confidential may arise for many different reasons. For example, the information may be proprietary, intended only for entity personnel.

Confidentiality is distinguished from privacy in that privacy applies only to personal information, whereas confidentiality applies to various types of sensitive information. In addition, the privacy objective addresses requirements regarding collection, use, retention, disclosure, and disposal of personal information. Confidential information may include personal information as well as other information, such as trade secrets and intellectual property.

Privacy

The privacy criteria are organized into eight categories:

- *Notice and communication of objectives.* The entity provides notice to data subjects about its objectives related to privacy.
- *Choice and consent.* The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to data subjects.
- *Collection.* The entity collects personal information to meet its objectives related to privacy.
- *Use, retention, and disposal.* The entity limits the use, retention, and disposal of personal information to meet its objectives related to privacy.
- *Access.* The entity provides data subjects with access to their personal information for review and correction (including updates) to meet its objectives related to privacy.
- *Disclosure and notification.* The entity discloses personal information, with the consent of the data subjects, to meet its objectives related to privacy. Notification of breaches and incidents is provided to affected data subjects, regulators, and others to meet its objectives related to privacy.
- *Quality.* The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet its objectives related to privacy.
- *Monitoring and enforcement.* The entity monitors compliance to meet its objectives related to privacy, including procedures to address privacy-related inquiries, complaints, and disputes.

Trust Service Categories and Related Control Activities

Integration with Risk Assessment

Along with assessing risks, WellSky's management has identified and put into effect the necessary actions to address those risks. In order to address these risks, control activities have been placed into operation to help ensure that the actions are carried out in a competent and efficient manner. Control activities serve as various mechanisms for managing the achievement of the security, availability, processing integrity, confidentiality, and privacy principles and applicable criteria.

Selection and Development of Control Activities

The applicable trust criteria and related control activities are included in the control matrices, within Section 4 of this report, to eliminate the redundancy that would result from listing the items in this section as well. Although the control activities are included in the testing matrices set forth below in Section 4, they are, nevertheless, an integral part of WellSky's description of its Healthcare Solutions and Advisory and Outsourced Services Systems. Any applicable trust services criteria that are not addressed by control activities at WellSky are also described within the control matrices.

Information Systems and Communication

Information Systems

WellSky's corporate systems reside within the TierPoint, Kansas data center and are protected by physical and logical security controls to ensure equipment and information is protected from unauthorized access. The production and backup servers are housed at multiple cloud hosting and data center facilities. WellSky relies on the physical and logical access controls of each cloud hosting and data center hosting provider to protect equipment and information from unauthorized access.

Customer data and transaction information recorded on WellSky's systems are backed up according to management's backup policy. Backup procedures are in place to ensure that backed up data is secure, available, and verified for the integrity of data to ensure recovery in the event of a failure to primary production systems. Environmental monitoring technology, along with fire suppression devices are monitored by the management and staff of the contracted data centers to help ensure production equipment is protected and issues are identified in a timely fashion.

Confidential data transmitted through WellSky Solutions is secured and protected using various access control mechanisms. Customizable services and reports are available to meet the specialized needs of clients as well as automated order and delivery options via the web or direct computer communications.

Communication

Management is involved with day-to-day operations and is able to provide personnel with an understanding of their individual roles and responsibilities. This includes the ability to provide necessary training to the extent that personnel understand how their daily activities and roles relate to the overall support of services. WellSky's management believes that open communication throughout the organization ensures that deviations from standards are identified, reported, and appropriately addressed.

Monitoring

Monitoring is generally performed through active, hands-on management, including quarterly executive meetings to discuss operational issues. Executive Management is involved and active in the business. WellSky utilizes a risk-based approach to monitor business units and other entities throughout the organization, ensuring that enterprise-wide risks are prioritized and addressed in order of significance. Results from the risk evaluation are documented in formal communications to Executive Management and other relevant parties.

WellSky monitors customer communications through the help desk ticketing system. This information is provided to the system administrators, providing the ability to track, monitor and assist in understanding customer complaints or concerns, and to evaluate and resolve special requests in a timely fashion. Management's ability to actively monitor customers' communications is integral to controlling the quality of the services provided.

WellSky's monitoring procedures include:

- Internal and external automated system in place to provide availability and performance statistics for review by technical staff and management.
- Analysis of, and appropriate follow-up on, operating reports or metrics that might identify anomalies indicative of a control failure.
- Supervisory reviews of internal control.
- Notifications and alerting for any monitoring issues.
- Quarterly user access reviews for monitoring user permissions and rights within the system.

User Entity Controls

The control activities performed by WellSky cover only a portion of the overall internal control structure of WellSky's user entities. Therefore, each customer's internal control structure must be evaluated in conjunction with WellSky's control policies and procedures described in this report. WellSky's controls over its Healthcare Solutions and Advisory and Outsourced Services Systems were designed with the understanding that certain user entities controls were in place and operating effectively.

Complementary User-Entity Controls	Related Applicable Trust Criteria
User entities are responsible for immediately notifying WellSky of any actual or suspected information security breaches, including compromised user accounts.	CC2.3
User entities are responsible for notifying WellSky of any approved contact modifications.	CC6.2
User entities are responsible for management of user access requests through the use of a formal request form provided to WellSky to ensure appropriateness of access to their storage locations on the WellSky network and applications.	CC6.2
User entities are responsible for ensuring that user IDs and passwords used for accessing WellSky systems are assigned only to authorized individuals and that the roles assigned to the user account are appropriate.	CC6.2
User entities are responsible for ensuring the confidentiality of any user accounts and passwords assigned to them for use with WellSky's Healthcare Solutions and Advisory and Outsourced Services Systems.	CC6.2
User entities are responsible for maintaining their own system of record of data files provided to WellSky.	PI1.2
User entities are responsible for ensuring the completeness and accuracy of system inputs.	PI1.2
User entities are responsible for providing data in an appropriate and approved format to WellSky for processing.	PI1.3
User entities are responsible for notifying WellSky of any data modifications required.	PI1.3
User entities are responsible for monitoring the completion of data transfers to WellSky.	PI1.3
User entities are responsible for providing WellSky data in accordance with their corporate confidentiality policies.	C1.1
User entities are responsible for notifying WellSky of any potential breaches of confidential information.	C1.1, C1.2
User entities are responsible for using the secure methods provided by WellSky to facilitate confidential data transfer.	C1.2
User entities are responsible for complying with their notice of consent and privacy requirements when transmitting data to WellSky and other organizations.	P1.1, P2.1, P6.1
User entities are responsible for immediately notifying WellSky of any actual or suspected information security breaches, including compromised user accounts.	P5.1
User entities are responsible for notifying WellSky of any potential breaches of confidential information.	P5.1
User entities are responsible for notifying WellSky of any approved contact modifications.	P7.1

MARCUMGROUP

Marcum Group is a family of organizations providing a comprehensive range of professional services including accounting and advisory, technology solutions, wealth management, and executive and professional recruiting.

These organizations include:

- Marcum LLP
  www.marcumllp.com
- Marcum Bernstein & Pinchuk
  www.marcumbp.com
- Marcum Insurance Services
  www.marcumis.com
- Marcum RBK Ireland
  www.marcumrbk.com
- Marcum Search
  www.marcumsearch.com
- Marcum Strategic Marketing
  marketing.marcumllp.com
- Marcum Technology
  www.marcumtechnology.com
- Marcum Wealth
  www.marcumwealth.com

MARCUM
ACCOUNTANTS ▲ ADVISORS

Ben Osbrach, CISSP, CISA, QSA, CICP, National Risk Advisory Leader
813.397.4860 ● ben.osbrach@marcumllp.com

Mark Agulnik, CPA, CISA, CIS LI, JD, Regional Advisory Partner-in-Charge
954.320.8013 ● mark.agulnik@marcumllp.com