dedicated to our clients

Disaster Recovery as a Service
KeyCloud

AppleCare Medical

December 2, 2016

30077 Agoura Court, Agoura Hills, CA 91301
Toll Free: 877.442.3249 P: 818.992.8950 F: 818.992.8970
www.keyinfo.com

1. Disaster Recovery as a Service (DRaaS) Terms

1.1 General Terms – Client agrees that it is solely responsible for all activities that occur under Client's accounts, regardless of whether the activities are undertaken by Client, Client's employees or third parties (including Client's contractors and agents), and KeyInfo is not responsible for unauthorized access to Client's account unless such unauthorized access is solely due to the actions or inactions of KeyInfo. Client agrees to comply with all applicable laws and regulations applicable to, and/or affecting, Client's access and use of the Managed Hosting Services, and KeyInfo shall not have any responsibility to Client therefore including, without limitation, any responsibility to advise Client of Client's responsibilities in complying with any laws or regulations affecting Client's use of the Managed Hosting Services. Client may not resell any of the Managed Hosting Services without the written consent of KeyInfo, which written consent may be set forth in the applicable SOW. Subject to the foregoing, if Client resells any Managed Hosting Service, Client shall require its customers and end users to comply with any laws or regulations affecting Client's use of the Managed Hosting Services. The Parties agree to (a) cooperate with reasonable investigations of outages and security problems with respect to any Managed Hosting Services and any suspected breach of this Agreement, (b) immediately notify each other of any unauthorized access to, or use of, the Managed Hosting Services or any other breach of security, and (c) not to take any action or install any software which may preclude or impair KeyInfo's ability to access or administer its servers and Client's ability to access to the Managed Hosting Services.

1.2 Description – KeyInfo works to ensure successful and timely restoration of all Client data that it provides Disaster Recovery services for. The system will replicate Client data in accordance with selections the Client makes during the provisioning process. KeyInfo only guarantees the system will replicate any customer data on or off of the Client's premises that is identified in this SOW. KeyInfo will actively monitor the status of replication, attempt to resolve any issues that occur with replication, and contact Client if their intervention is required. Client shall report to KeyInfo any errors in executing such replications promptly by web submission, email or telephone. KeyInfo will provide Client with the ability to view the condition of the overall replication status via the web based interface or other tool. It is the Client's responsibility to verify that the Client data the Client intends to replicate is accurately reflected in the web based interface and is being replicated by the system and reporting no errors.

1.2.1 Successful Replication or Notification – KeyInfo will notify Client of any critical failed replication operation as agreed upon. Client is solely responsible for insuring that KeyInfo has the proper, up to date, contact information.

1.2.2 Time to Initiation of Restoration – Client has full control to initiate a full or partial restoration in accordance with the terms of the underlying contract. KeyInfo will initiate Client data restoration within the Recovery Time Objective (RTO) as indicated. The Client is responsible for integrity of Data targeted for replication by KeyInfo. KeyInfo backs up data "as is, where is" and will restore data in the same format in which it is replicated. (Example: corrupted data will get backed up replicated and restored in the same state.)

1.3 Service Level Definitions

1.3.1 Successfully Replicated Data – KeyInfo can only provide 100% data recovery guarantee on the data that has been backed up between the Client's server and the Data Center without error. Key Info will continuously replicate data in recurring cycles and notify the Client in the event of an error in the replication process. In the event of a replication failure KeyInfo will contact Client to arrange for a subsequent repair.

1.3.2 Data Restoration Initiation – In most cases a Client will be able to restore files without KeyInfo assistance. Where necessary, the Measured Time to Begin Data Restoration starts upon notification of a data restoration by the Client to the KeyInfo Network Operation Center by telephone, in accordance with this Agreement, and the release of the affected service by the Client to KeyInfo for executing a data recovery. The measured time to restore ends when the data recovery is completed. KeyInfo will notify the Client by telephone and Client will confirm that data recovery has been initiated.

1.3.3 Recovery Point Objective (RPO) – Data replication occurs at a fixed point in time according to a schedule agreed upon between KeyInfo and Client. Any data that exists between replication cycles is vulnerable. The length of time between replication cycles is the RPO. This is the point back in time to which a Client's data must be recovered.

1.3.4 Recovery Time Objective (RTO) – This is the maximum elapsed time required to complete the recovery of Client's data. RTO is a function of the size of the data delivery circuit and the total amount of data to be recovered. RTO objectives should be discussed with KeyInfo account executive. An RTO measurement will begin only when a customer environment is properly functioning and ready to receive data. The approximate RTO will be impacted by the technology utilized for the recovery solution.

1.4 System Maintenance. Client Maintenance includes the installation of hot fixes, service packs, software and software upgrades, preemptive hardware replacement, and hardware upgrades to infrastructure that is not shared with other Clients. Client will be notified in advance of a Scheduled Client Maintenance event in accordance with the Notification and Escalation procedure ("NEP") unless specifically agreed to otherwise. Notification will take place via email and telephone phone call to Client's technical contact. Notwithstanding anything contained in this SLA to the contrary, remedies in this SLA do not apply to outages that result from Scheduled Client Maintenance conducted pursuant to and in accordance with this Agreement. KeyInfo reserves the right to perform emergency maintenance without prior notice to Client (although KeyInfo shall use commercially reasonable efforts to provide such prior notice) under the terms of this SLA if the maintenance is reasonably necessary to maintain the security of any of the infrastructure hosted by KeyInfo; provided, however, that KeyInfo shall promptly notify Client after any such emergency maintenance is performed, and such notice to be given within four (4) hours after discovery of the security issue giving rise to the emergency maintenance. Notwithstanding the foregoing, outages that are caused by any KeyInfo maintenance that is not Scheduled Client Maintenance, including, without limitation, emergency maintenance, shall

constitute an outage and shall be included in the calculation used to determine any service credits that Client may be entitled to under this SLA.

1.5 Scheduled Maintenance Windows. Scheduled Maintenance Windows are scheduled, when necessary, a minimum of seventy-two (72) hours in advance. The purpose of a Scheduled Maintenance Window is to perform maintenance activities to shared infrastructure, such as changes or upgrades to core routing or switching equipment, SAN, or other data center facilities. Notifications of Scheduled Maintenance Windows are sent via email to all Client contacts on record. Scheduled Maintenance Windows shall occur no more frequently that once per month, without Client's prior written consent, and shall only be during off-peak hours (9:00 P.M. to 4:00 A.M. Pacific Time). Notwithstanding anything contained in this SLA to the contrary, remedies in this SLA do not apply during performance of maintenance activities conducted during Scheduled Maintenance Windows and in accordance with this Agreement.

Appendix A – Data Center Specifications

1) Data Center Critical Infrastructure

a) Physical Security

i) Access Control and Surveillance. Access to the Key Info data center is strictly controlled with two factor biometric security scanners and proximity access cards. All entrances accessible to Clients are monitored via CCTV cameras and all entrance/exit activity is digitally recorded.

ii) Manned Operations. KeyInfo data center personnel support the data center 7/24/365 to respond to critical events, emergences, and to provide support.

iii) Client Access. Upon reasonable notice to KeyInfo or in cases of emergency, Client shall be granted access to the Facility. Client access to the KeyInfo data center is strictly limited to those areas designated for Colocation Floor Space, Server Colocation services, and areas housing any Client Equipment only. Client access to Managed Hosting portions of the data center is not permitted. Authorized KeyInfo data center personnel will accompany Client at all times while inside the data center.

iv) Public Access. Public, non-Client access to the data center is limited to the KeyInfo Business Partner Innovation Center portion of the data center and certain designated viewing areas and will be escorted at all times. Public access to any other portion of the data center, including all areas where Client equipment is located, is strictly forbidden. Authorized KeyInfo data center personnel will accompany visitors at all times while inside the publicly accessible portions of the data center.

v) Fire Protection. The KeyInfo data center is equipped with comprehensive fire detection and suppression systems. The service level objective is to prevent and suppress potential causes of fires using early detection systems

b) Power Availability

i) Power Uptime. The data center power systems are designed to provide uninterrupted power, regardless of the availability of power from the local public utility(s) supplying the data center.

ii) Power Services. AC power to the rack(s) or cabinet(s) housing Client Equipment is guaranteed to be available 99.999% of the time in a calendar month. For Client to properly make use of this benefit, Client Equipment must either be equipped with dual power cords or, if single-corded, attached to an automatic transfer switch ("ATS") within the Client rack(s).

c) Cooling and Climate Control

i) A/C services. KeyInfo guarantees that adequate cooling and humidity control (climate control) will be provided 99.999% of the time in a calendar month. The ambient temperature in the Managed Hosting, Server Colocation and Colocation Floor Space areas of the data center that are four (4) feet above the ground and surrounding the Client Equipment will be 72 degrees Fahrenheit +/- 5 degrees; provided, however, that such temperature guarantee shall not apply if any rack housing Client Equipment consumes more than 5kWs. Relative humidity within these same areas will be 40% +/- 5%.

ii) Key Info may request access for the implementation and/or modification of energy saving and efficiency measures in the data center, with client permission.

d) Network Infrastructure

i) Network Availability. The KeyInfo network infrastructure is guaranteed to be available 99.999% of the time in a calendar month. The applicable portion of the infrastructure is specific to the type of connection provided and includes all relevant switches, routers and cabling. KeyInfo provides Internet bandwidth, and also allows Clients to extend their private networks to the data center. Internet bandwidth is brought directly to the Client rack. Private networks may be extended to the Client rack via carrier circuit extension from the data center demarc or via cross-connect from a carrier point-of-presence ("POP") already residing in the data center ("on-site carrier").

ii) **Carrier-installed circuit extensions or other circuits or connections not installed or owned by KeyInfo are not covered under this SLA.**

iii) For services using KeyInfo provided Internet bandwidth, the network infrastructure is defined as the portion of the network extending from the outbound switch port at the Client rack to the outbound port on the KeyInfo border router.

iv) For services using Client-provided private bandwidth with a cross-connect to an on-site carrier, the network infrastructure is defined as the portion of the network extending from the outbound port at the Client rack to the outbound port of the carrier's POP. Cross-connections installed by KeyInfo are guaranteed to be available 100% of the time a calendar month.

v) Network Availability is defined as the ability to pass TCP/IP traffic with less than 0.5% packet loss and less than 30ms latency across the KeyInfo network infrastructure. Network downtime is defined as the amount of time that Network Availability is below 100%, and is measured from the earlier of the time a support ticket is opened or notification is received from Client.

vi) Internet Availability. KeyInfo obtains Internet bandwidth from multiple providers in order to deliver the highest level of availability. KeyInfo guarantees that Internet connectivity will be available 99.999% of the time in a calendar month.

vii) Internet Availability is defined as the ability to pass TCP/IP traffic from the KeyInfo border router to an upstream Internet provider. Internet downtime is defined as the amount of time that Internet Availability is below 99.999%, and is measured from the earlier of the time a support ticket is opened or notification is received from Client.

viii) Internet Bandwidth. KeyInfo will initially provide Client the amount of bandwidth specified on the Services Agreement. Bandwidth may be increased or decreased at any time upon written request from Client. Bandwidth changes may result in changes to Client's Monthly Recurring Charges and are subject to approval by Client and KeyInfo prior to implementation. Bandwidth decreases will be processed within one (1) business day of approval by both parties. Bandwidth increases will normally be processed within one (1) business day of approval of both parties provided that KeyInfo has the additional bandwidth available, otherwise it will be processed within one (1) business day after KeyInfo obtains additional bandwidth from its upstream providers.

ix) Third Party Penetration Testing and Vulnerable Assessment. In addition to real-time security tools, KeyInfo employs a third-party security company to provide comprehensive penetration testing services and provide full security assessments. A report on all potential vulnerabilities in the KeyInfo network is provided, and along our team, an immediate remediation plan is implemented to address concerns that are identified.

x) IP Addresses. KeyInfo will assign public IP addresses to Client at commencement of the Services.

xi) Firewall Security and IDS/IPS Security. KeyInfo has established a firewall system that restricts access to KeyInfo's infrastructure between the external access points and internal network. DMZ's are in place at the web server layer to further isolate external traffic from the internal network. KeyInfo utilizes advanced firewall technologies from Cisco to ensure security at multiple layers in the OSI stack. Further, we use sophisticated monitoring software for DNS and IP traffic conversations, along with other protocol analysis tools. We use next generation Intrusion Detection and Intrusion Prevention tools to detect and remediate security threats before they happen.

2) IT Equipment

i) **Virtual Server Infrastructure.** KeyInfo has built a virtualized server environment based on technology from several major manufacturers. Virtual servers may be provided to Clients as part of the Managed Hosting Service. KeyInfo guarantees the availability of its virtualized server infrastructure, and will redeploy virtual servers as necessary should an underlying physical server fail. Upon the failure of a physical server supporting a set of virtual servers, a KeyInfo technician will ensure that all affected Client virtual servers are restored to operational status on another physical server within the virtualized server environment. "Operational status" means that the virtual server has been restarted and responds to an ICMP "ping" on its Client facing network interface. The restoration to operational status is guaranteed to be complete within one (1) hour after failure detection by KeyInfo. This guarantee excludes the time required to restart applications during a recovery.

ii) **Storage Area Network Availability.** The KeyInfo data center features a Storage Area Network (SAN) built with storage hardware from leading enterprise storage vendors. The SAN is fully redundant across all components and is virtualized to provide high levels of performance and availability. All components have redundant power supplies and redundant fiber connectivity. The switch fabric is built with fully redundant hardware, dual fiber paths and dual host-bus adapters in each connected server. The logical disk arrays are constructed using industry-standard RAID data striping techniques and online hot-spares. In the event of a failure that renders the SAN unavailable, KeyInfo will repair the SAN within one (1) hour of the time that the cause of the problem is identified (which KeyInfo shall use its best efforts to determine). SAN downtime is defined as the amount of time that Client equipment is unable to transmit or receive data on the SAN, and is measured from the earlier of the time a support ticket is opened or notification is received from Client.

3) Monitoring and Response

i) **Monitoring.** Monitoring services are included in the disaster recovery SOW. This monitoring includes verifying the state of replication as well as the health of the target DR virtual and supporting infrastructure. The health of the replication will

include the state of the connectivity between Key Info and the Client, that replication relationship is active between Client and Key Info, and that Recovery Point Objectives are within the specified limits.

ii) **Response.** When alerted of a potentially critical problem by any of its monitoring systems, KeyInfo will begin troubleshooting and addressing the problem and will contact the Client using the defined Notification and Escalation procedure according to response time matrix shown below. Key Info staff is notified through a mix of technologies including email, SMS, and telephone. Client-initiated support tickets – Upon entry of a support ticket in the KeyInfo Problem Management System by Client, either by telephone call to the KeyInfo Network Operations Center or via online web portal, KeyInfo will respond according to the response time matrix shown below.

iii) **Response Time Matrix**

Severity/Priority Level	Response Time	Support Coverage	Example
1 Service down	30 Minutes	24/7	A server or application is not accessible to users
2 Improper operation or degraded performance	Within 1 hour	24/7	A server or application is accessible, but not function correctly or responding poorly.
3 Non-critical	Within 4 hours	24/7	Operational or technical assistance is requested for infrastructure services or scheduling of a maintenance outage, or need help with any other non-immediate task.
4 Low priority	One Business Day	8/5	A basic configuration change is requested.

dedicated to our clients

Appendix D – Key Cloud – Statement of Work

1) **Project Leaders.** Leaders who are responsible for, and be the principal point for contact for, communications with the other party regarding the subject matter of the Statement of Work.

	Key Information Systems	CLIENT
Project Lead	**Clayton Weise** **Director Cloud Operations** **cweise@keyinfo.com**	**Sean Igarta** **Manager of Technology Services** **Sean.igarta@applecaremedical.com**
Account Management	**Todd Smith** **Account Executive** **tsmith@keyinfo.com**	

2) **Connectivity.** The following connectivity will be provided:

Connectivity	
Internet Bandwidth (Mb): • KeyInfo will provide eight (8) public IP addresses at the commencement of service. Additional public IP's are available at additional charge and with valid justification. • Committed and burst rates may be increased at any time according to the terms defined in the SLA.	
VPN information	
Private Bandwidth Description	
Carrier(s)	
Service Description • Service type (e.g. MPLS) • Total number of circuits • Failover configuration	**Key Info IP/DIA**

3) Managed Servers

Server Description	Specifications
All Managed Servers and Virtual Instances include: • Operating System • 24/7/365 Operations Support • Fault Monitoring • Operating System Patching (Non-LPPs)	**Not Included**

4) Monitoring and Operational Support Services

Monitoring • Basic Port Monitoring with 5 Minute Polling • URL Availability[1] (text string matching on 1 URL, checks the site every 10 minutes) • Support Ticket Creation, Automated Alert Escalation and Client Notification • Collection and reporting of performance metrics (CPU, memory, disk, network, etc.) for supported devices • Threshold monitoring and Automated Alerting • Replication status	**Included**
Network Device Management • Basic configuration and administration of supported devices • Software updates to supported devices	**Included**
Patching • Hypervisor • Firmware	**Included**
Server Administration • Administration of user accounts, file system and print queues.	**Not Included**
The KeyInfo Technical Operations Center (TOC) serves as the focal point for all monitoring and support services	

5) Description of Services- Pricing

DR Environment will be provisioned at Phoenix Data Center:
3402 E. University Dr., Phoenix, AZ 85034

roduct	Description	Qty	Unit Price	Ext. Price
CLD-X86-CORE-DR	Intel vCPU Cores (standby)	60	$3.50	$210.00
CLD-X86-RAM-DR	Intel vRAM (per GB, standby)	128	$3.00	$384.00
CLD-ZRTO-VM	Zerto replication license (per VM)	10	$75.00	$750.00
CLD-MON-WIN	Cloud monitoring (Windows, per VM)	10	$50.00	$500.00
CLD-STOR-DR	Disk Storage (per TB) Standby	20	$75.00	$1,500.00
DR Resource Summary				$3,344.00
One-time Fees				
SPG-SOW	Professional services work	1	$3,000.00	$3,000.00
CLD-DR	Disaster Recovery Declaration	-	$5,000.00	$5,000.00
CLD-DRTEST	Key Info assisted DR test (6 semi-annual tests over course of engagement)	-	$10,000.00	$10,000.00
Billing Summary				
			Monthly Rate	$3,344.00
			Setup and Testing Fees	$13,000.00

dedicated to our clients

Terms

- The term of these options is **36 months** and will be billed up-front for a total of $133,384, unless otherwise noted
- Services must be terminated with 90-day notice in writing
- If services are terminated early, the remaining amount afer 90 days will be returned to Client
- Total term payment **excludes** declaration costs, DR execution is billed upon completion
- Contract will start upon a date agreeable to both parties based after the installation and initial testing/validation of the DR service
- Applications included in this SOW are the critical Tier 1 applications as specified by Client
- Data will be transmitted via encrypted VPN and stored encrypted at rest
- After 5 days of runtime during a disaster declaration production will be billed in accordance with the table below

SKU	Description	Unit Price
CLD-X86-CORE	Intel vCPU Cores	$14.00
CLD-X86-RAM	Intel vRAM (per GB)	$12.00
CLD-STOR	Disk Storage (per TB)	$100.00

30077 Agoura Court, Agoura Hills, CA 91301
Toll Free: 877.442.3249 P: 818.992.8950 F: 818.992.8970
www.keyinfo.com

dedicated to our clients

By signing below, Client and KeyInfo agree to be bound by this Agreement.

Key Information Systems, Inc.	**Client**
BY:_____	BY:_____
NAME:_____	NAME:_____
TITLE:_____	TITLE:_____
DATE:_____	DATE:_____

30077 Agoura Court, Agoura Hills, CA 91301
Toll Free: 877.442.3249 P: 818.992.8950 F: 818.992.8970
www.keyinfo.com