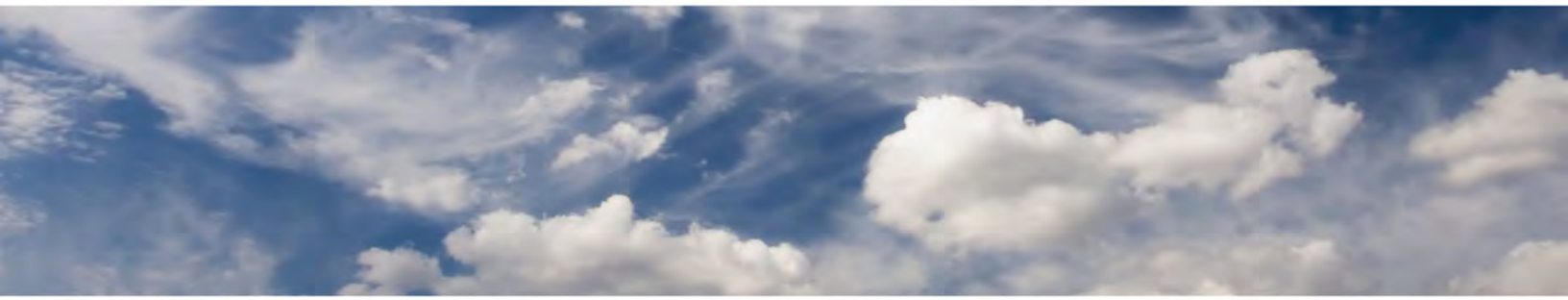
The Medikin Dictation System



The Medikin Dictation System (MDS) is a cloud based dictation system which enables clinics, law firms, transcription companies and more to have an advanced and flexible dictation solution at very low cost.

The Medikin Dictation System provides an ideal self-managed solution for our clients. Although the system is managed and supported by Medikin at the IT infrastructure level by Medikin the client can add and remove users at any time via the web based control panel.

These are some of the benefits that are enabled with the MDS:

- The MDS is customizable, stable and secure
- Dedicated DID's or toll-free numbers can be provisioned per law firm, clinic, etc. which enhances security and enables branding and provisioning of preferred login IDs that may not be available on monolithic systems
- Provisioning custom branded outbound welcome greetings per toll-free
- Provisioning logins and passwords of arbitrary length
- Quick or instant turnaround time to add new accounts

Technical Specifications
Servers, Redundancy...

Medikin developed its custom software to run on an open source stack consisting of Asterisk, Linux, Apache and mySQL. You can rest assured that the most trusted, tested and stable open source technologies are the foundation of the MDS.

PHYSICAL SERVERS
Medikin's servers are powered by quad-core Intel Xeon processors with multiple hot-swappable hard drives in RAID 1 configurations and dual power supplies. KVM-over-IP enables systems administrators to remotely access the servers at the BIOS level in case of any critical server issues.

VIRTUAL SERVERS
Medikin utilizes the open source Xen Hypervisor virtualization technology to provision services to its clients via virtual servers running the latest stable version of the Debian distribution of the Linux open source operating system. Virtualization enables Medikin to scale up very quickly and without interruption to existing services. Virtualization provides many other benefits such as mirrored standby servers, datacenter flexibility, more efficient use of computing resources and greater application security.

HIPAA COMPLIANT CLOUD COMPUTING
Medikin elected to build and operate its own private cloud computing infrastructure in order to maintain strict HIPAA compliance. Outsourcing to a typical cloud computing vendors may not be HIPAA compliant due to the fact that they stripe the data and applications of their various clients across a shared server infrastructure which obscures the verifiability of the privacy of their clients' data.

SYSTEMS MONITORING
Physical and virtual servers as well as critical services are monitored 24X7 by a customized implementation of the open source Nagios monitoring software. Alerts are sent to qualified on-call engineers via email and SMS.

TICKETING AND BUG TRACKING
Medikin uses OTRS and Bugzilla for online trouble ticket management and bug tracking. These are open source tools which enable us to support our clients effectively while maintaining a searchable archive of issues that aids in the debugging and further development of the code base.

DATABASE SYSTEMS
The databases reside on servers dedicated exclusively for reading from and writing to the database tables. Multiple database servers handle the active client data, and standby servers are updated nightly to provide fault tolerance at the database processing layer. Medikin utilizes the most advanced open source database software MySQL and the AFS file system for enhanced security, scalability and efficiency.

Technical Specifications

Data Center, Archives...

DATA STORAGE

All client audio data as well as virtual server image and code repository updates are backed up to a storage system consisting of a large redundant array (RAID 5) of hot-swappable disks which stripe the data across the drives to ensure continuity in case of a disk failure. A secondary incremental backup is transmitted nightly via VPN to a storage server in Medikin's secondary datacenter. Off-site backup to fixed media such as tape or DVD is available upon request.

DATACENTERS

Medikin's primary datacenter is a SAS-70 Type II accredited datacenter which provides secure and reliable rackspace via tight physical security, advanced environmental controls and redundant sources of utility, battery and diesel generated power. Medikin's IP network is managed by Internap's patented route optimization technology which intelligently routes data across multiple Tier-1 Internet backbones, insulates traffic from network outages and provides low-latency connectivity, dynamically identifying optimal paths for business-critical data. Internap provides Medikin with the highest possible uptime guarantee and 24X7 direct access to certified network engineers. The aggregated features of the datacenter facility, Internap's operational support and Medikin's own monitoring systems include:

- 24X7 Physical Site Monitoring
- Security: Access Card, Fingerprint Scan, Video Surveillance, On-duty Patrol
- Backup Power: Redundant Uninterruptible Power Supply Battery Banks
- Diesel Generator for continuous supply of al ternate backup power
- Diesel Fuel Reserve: 2 days, with multiple ven dors on call
- Fire Protection: Pre-action Sprinkler with Inte grated Smoke Detection System
- Floors: Slab with overhead cable trays
- Secure vented cabinets with dual locks for Medikin servers
- Redundant cross-connected Gigabit switches
- Redundant 20 AMP power from distinct utility power sources
- Redundant power supplies in servers to re ceive power from distinct power sources
- Redundant Domain Name Servers
- Redundant 100 Mb Internet connections via Internap's route optimized Internet access
- 100% Uptime Guarantee for Power and Inter net
- 24X7 Server Monitoring with SMS Notification
- 24X7 access to Internap's Network Operations Center
- 24X7 access to Medikin's Systems, Network and Coding Engineers

Technical Specifications

Security, Trust...

SYSTEMS SECURITY

Medikin employs a variety of systems security measures including:

- Using the Debian Branch of Security-Enhanced Linux
- Hardened Wrapper Deployment via DenyHosts Blacklisting
- Whitelisting that limits access to servers that re quire access from a limited set of addresses
- Automatic Security Updates With Rollback Fail safe
- Rootkit Defense via Rootkit Hunter
- Host Based Intrusion Detection
- Password Rotation Schema

APPLICATION SECURITY

User access to Medikin is secured via:

- Unique user IDs and passwords
- Logged and verified ID modifications
- Access privileges associated by username
- Transmissions made via SSL or Secure FTP

TRANSMISSION SECURITY

Medikin secures the transmission of audio files via 256-bit SSL encryption. All the access points to audio files are identified and authenticated by a username and password combination.

TRUST

Confidentiality of client data and Protected Health Information (PHI) is of prime importance to Medikin. As a provider of outsourced IT services to its clients Medikin provides a HIPAA compliant Software-as-a-Service by adopting the aforementioned security measures. But technical measures are not sufficient. Medikin employees sign a confidentiality agreement which addresses the confidentiality of PHI, and are nonetheless restricted in their access level according to the requirements of their roles.

EXPERIENCE

Medikin's technologists have many decades of experience in Network Security, Telecommunications and the design, development and support of mission critical applications. Medikin maintains a "Five 9's" – 99.999% uptime track record.