Nightingale Notes is a web-based, hosted software as a service (SaaS) solution. Nightingale Notes is a full electronic health record (EHR) capable of documenting client encounters from intake to billing and discharge. No installation is needed. Our public servers are hosted by Amazon Web Services (AWS).

Application Platform

Nightingale Notes is written in an open source language called Ruby on Rails and the database backend is powered by an open source database server called PostgreSQL.

System Integration

Nightingale Notes is able to transfer data to other application platforms that allow data import (not real-time synchronous exchange). This can be achieved by exporting the data out of Nightingale Notes in .xml format or .csv format. An output file can then be manipulated (parsed) by the agency to conform to the import standards of the other software platform.

System Hardware Recommendations

Nightingale Notes is a web-based, hosted solution; there are no specific hardware requirements. Our recommendations for optimal performance are below:

- Internet connection with port 443 open for SSL
- Pentium 4 or newer processor that supports SSE2
- Minimum 2GB of RAM
- Computer, laptop, or tablet: Champ will support any tablet that can run the full version of Chrome, or Safari. Please note when selecting tablets or mobile devices that a full version Windows must be installed so that a full version of the browser can be run. Some tablets run portable versions of Windows, which means that the install of the browser may not be the full version, resulting in possible issues.

System Software & Internet Connection Requirements and Recommendations

Because Nightingale Notes is a software as a service (SaaS) product, no installation is required. To run Nightingale Notes, the only requirements are the latest version of Safari, Chrome.

We recommend a high speed internet connection (3Mbps or greater) for office environments which need to support more than a single user accessing the internet at once. While in the field you can access the application using a cellular data connection. Cellular data connections typically have speeds of at least 32Kbps which is sufficient for the work that is done in the field. A comparison between a 3Mbps connection and a 32Kbps connection shows a negligible difference in the time it takes to access a client's chart.
Accessing a client's chart consists of:

1. Logging in
2. Doing a search for the client

3. Listing the client's activities
4. Viewing the chart for an activity

Using a 3Mbps connection this process takes ~ 20 seconds and using a 32Kbps connection this process takes ~ 30 seconds.

Server & Security Reliability

Our public servers are hosted by AWS in their data centers. AWS carries numerous certifications which can be accessed in their "Amazon Web Services Risk and Compliance" whitepaper. Nightingale Notes runs on dedicated instances, per HIPAA requirements.

AWS has many years of experience in designing, constructing, and operating large-scale data centers. This experience has been applied to the AWS platform and infrastructure. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. Automatic fire detection and suppression equipment has been installed to reduce risk. The data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, seven days a week.

AWS utilizes a wide variety of automated monitoring systems to provide a high level of service performance and availability. AWS monitoring tools are designed to detect unusual or unauthorized activities and conditions at ingress and egress communication points. These tools monitor server and network usage, port scanning activities, application usage, and unauthorized intrusion attempts.

All customer data in Nightingale Notes is encrypted at rest and in transit using industry standard cryptography.

Backup & Disaster Recovery

Using AWS as a hosting provider simplifies backup and disaster recovery scenarios, due to their built-in capabilities and extensive network of data centers. File attachments in Nightingale Notes are automatically replicated in multiple data centers. The database is backed up incrementally minute-by-minute, with base backups occurring nightly. Database data is stored in geographically distinct data centers, on the East and West Coasts. If you would like to have a backup stored in your office or another location to which you have access, a weekly secure transmission of your agency’s backup can be arranged.

In the case of a disaster rendering a datacenter unreachable, or destroying hardware completely, AWS's consistency in infrastructure allows new servers to be provisioned quickly in a different geographical region. Server and network configurations (including encryption and access control policies) are templatized, minimizing the amount of manual effort and potential delays in restoring Nightingale Notes for service.

Disaster recovery simulations are conducted monthly by executing a script that launches and configures servers, bringing them online with an up-to-the-minute database backup, in a West Coast datacenter. (Production servers are in an East Coast datacenter.) This process typically completes in under an hour. Obviously, actual disaster situations vary greatly in complexity. Recovery time will depend on the availability of AWS services, and AWS's ability to inform our decision to initiate failing over to a different datacenter. As of today, we have never encountered a situation meriting a fail-over discussion.

Other Incidents

Champ will notify an agency via certified mail if their data has been breached either through our physical or electronic property, or through that of a Business Associate, like AWS. This process includes assessing risk of a loss or potential unauthorized acquisition of client ePHI, and taking action when an actual loss or unauthorized acquisition occurs. It is the policy of Champ Software, Inc. to monitor, evaluate and assess risks of Information Security Breach events. It is Company policy to respond to any Information Security Breach event and to take appropriate action, notifying clients and third parties as required by law and contractual obligations and notifying law enforcement bodies when necessary or appropriate. Champ Software, Inc. will execute any necessary immediate mitigation immediately in the event of an Information Security Breach and as appropriate in the event of a Security Incident.

The CEO, CFO, and COO will be notified if it has been determined, or there is reason to believe, there has been potential access or acquisition of multiple customer/consumer ePHI by an unauthorized person such that assistance from outside law enforcement may be appropriate. If the CEO, CFO, and COO are notified pursuant to this policy, they will make an initial determination regarding whether an Information Security Breach has occurred requiring any notification pursuant to law or contract or whether any other notification is appropriate (e.g., law enforcement, clients per contractual requirements, consumers, or payment processors) under the circumstances depending on the nature of the Security Incident and the information at issue. This initial determination will be based on the following: applicable laws, contractual obligations, and other considerations including level of risk or potential harm involved and whether the matter should be reported to law enforcement.

System Maintenance & Upgrades

Nightingale Notes is regularly maintained and updated. Maintenance and updates are done seamlessly, behind the scenes. Because it is a SaaS, web-based solution, updates are automatic. When significant updates occur, users are notified of the release via email and a release meeting is held to go over new or improved features. For those unable to attend the release meeting, a recording and any notes from the meeting are sent out via email after the meeting is completed. In addition, release notes are available within the application upon login.

Nightingale Notes Support

Should the user experience any issues, support cases may be submitted by telephone, direct email, or a link on our website. Our Support staff is available by telephone from 8:00 am to 5:00 pm CT. Emails may be sent any time and are usually responded to within 2 business days. Support staff responds to most cases within 2 to 24 hours. In addition, we have online help available on every screen in the software and a Knowledgebase is available on our website.

Outages/Service Interruptions

In the event of an unplanned service disruption, Champ Software, Inc. sends our clients an email, including estimated time to service restoration, as soon as we are aware of the problem and then another email when service is fully restored. We have not had an instance where service was interrupted for even 30 minutes at one time. Interruptions to service are extremely rare and last less than a minute if they occur.

Application Security:

Since Nightingale Notes is a SaaS solution, no data is stored on local machines; all data is stored in the cloud. The software application is fully HIPAA compliant. All Champ Software, Inc. employees and subcontractors who work directly with our clients and their data have secure login credentials. In 2011, Champ Software, Inc. implemented background checks for new hires and all new hires must complete HIPAA training and receive the HIPAA training completion certificate if they will have access to client data.

If assisting our client requires accessing patient data then our client must set up a read-only access role and provide those login credentials to our employee. The client is instructed to inactivate or delete that login role once support concludes. An audit log within the Software logs every view, add, create, edit and delete action involving client-related ePHI in the application and can be accessed by agency administrators at any time to verify our support personnel are accessing only areas needed for troubleshooting purposes. Champ Software, Inc.'s written HIPAA Standard Operating Procedures may be provided upon written request and with a signed NDA.

All data in the application is encrypted at transit and at rest; all data is encrypted when transmitted from a public server to a client machine and vice versa using 256 bit SSL encryption. There are agency-level controls to set automatic record locking after a specified elapsed time. In addition, users can lock a record as needed manually.

An administrative user for each agency is supplied with a secure login and the ability to set up all remaining staff with appropriate roles and permissions. Roles within the application allow users to have read only, read/write, or read/write/delete to specific areas of the application including client information, activity level information, billing and claims, reporting and administrative functions. In addition, program assignments are used to further define and protect client data by allowing or stopping employees from accessing client records for highly confidential programs. All roles and programs can be defined by an agency to meet their needs.

Users are required and prompted to change their passwords every 90 days. Passwords must be at least 8 characters long and have at least 3 of the 4 following types of characters: lowercase letter, uppercase letter, number, non-alphanumeric character. User authentication protocol uses salted password hashing.

Audit Logging & Tamper Detection:

Database and application logs record all access and required actions. The Nightingale Notes application does not permit any changes to the audit log, ever. Only Champ Development Administrators have access to the database where audit logs are stored. This ensures that no changes are permitted via the application and that access to the backend is very limited to only authorized users.

There are only two system administrator level users who are authorized to access the system. Password requirements are: a minimum of 8 characters and a maximum of 128 characters including a minimum of three of the following mix of character types: uppercase, lowercase, numbers, and nonalphanumeric symbols. Additionally, we have multi-factor authentication for an extra layer of login security. There are also custom alarms set up in AWS to detect anomalies including failed login attempts, and changes to our custom AWS network or security policies.

In the application, new audit records are stored with a message digest. This is computed by taking the attributes of the record itself and concatenating those with the digest from the previous record to form a chain of records. A script is run monthly to verify that the stored values of the digests continue to match digests calculated from the data in the records. This verifies that the records themselves are unchanged and that the chain is unbroken.

Data Migration

When considering a migration from another software application, there are several factors that affect both the feasibility and the cost of the migration. They include:

- *Access to the data.* Without access to the data, no migration can occur.
- *Format of the data export.* The format used for the data affects the ease and cost of the migration. Several formats can be used: CSV, Database dump, copy of actual database files, XML, MS Access, Excel spreadsheet, etc.

- *Documentation of the data structure.* If documentation of the data schema can be obtained from the other Software vendor, the cost of the migration is reduced, and quality of the migration increased.
- *Quality of the data.* Some applications permit “bad” data to be entered, such as invalid dates. If the data to be migrated must be “cleaned” to remove invalid data, the cost of a migration increases significantly.
- *Integrity of the data.* For related tables it is important to have referential integrity in place. If there is no referential integrity in place, rules must be defined as to how to handle orphaned records, which will add additional time and cost to the migration.
- *Coding structures used in the other application.* Some data simply can’t be migrated because there is no comparable “concept” or term in our product.

Pricing for Data Migration

An accurate cost estimate of doing a migration cannot be determined in advance of a customer purchasing our product. An approximate estimate can be made if a prospective customer can obtain a data dump and documentation in advance, but such an estimate would be approximate only; it is impossible to know how many hours a migration will take until it has been started and is well along.

As a general rule, we recommend agencies assume only a basic set of data will be migrated – basic client demographics (see definition below), plus employee and physician data. This is due to the cost involved, and inevitable technical challenges. This will help an agency save the cost of keying basic data into the new system, although that cost may be more or less than the cost of a migration.

If an agency desires to explore a data migration beyond these guidelines, the cost of preparing an estimate will be added to the quote, and the estimate of the migration work itself will also be added to the quote, in a range of a minimum to a maximum figure. This is a two or three-step process. The first step would be a data dump with documentation. The second step would be making an estimate. The third step would be doing the migration. This will have many iterations while we work with agency staff to ensure the data is migrated as desired.

Basic Data Set

Given access to data, we can migrate client data that is stored directly in the clients table, excluding lookup values. This would include the following:

Field	Data Type	Size	Format
client_number	varchar	20	
opened_on	date	10	mm/dd/yyyy

born_on	date	10	mm/dd/yyyy
social_security_no	varchar	11	123-45-6789
medicaid_no	varchar	25	
medicare_no	varchar	25	
directions_to_home	text	Unlimited	
no_in_household	integer	2	
closure_on date	date	10	mm/dd/yyyy
discharge_note	text	Unlimited	
general_notes	text	Unlimited	
Occupation	varchar	50	
pre_pregnancy_weight	smallint	maxlength 4	
due_on	date	10	mm/dd/yyyy
delivery_on	date	10	mm/dd/yyyy
last_name	varchar	40	
first_name	varchar	20	
middle_initial	varchar	1	
suffix	varchar	4	
address_1	varchar	100	
address_2	varchar	100	
city	varchar	50	
state_code	char	2	
zip_code	varchar	5	
home_phone	varchar	25	
work_phone	varchar	25	
cell_phone	varchar	25	
illness_injury_pregnancy_on	date	10	mm/dd/yyyy
email	varchar	50	