Employee Health and Occupational Medicine
Technical Specifications
On-Premise Clients
Revised March, 2022

Table of Contents

Technical Requirements and Recommendations

This document explains the minimum requirements and provides recommendations to guide clients in implementing the software on their local area or wide area network infrastructure. These guidelines also outline additional options that are required to support special functions such as electronic signatures, scanning, auto-faxing and auto-emailing.

The specifications in this document are intended to serve as guidelines only. Individual implementation requirements may vary from these estimates on a case-by-case basis, depending upon the number of users, volume of transactions, type of network, and other software implemented on the same workstations, servers and network. Final decisions about hardware and networking technologies should be made by a qualified technical consultant, database administrator (DBA) or other qualified IT personnel.

General Overview

The software is a Microsoft® Windows™ based 32-bit application, designed to operate as a client in a Relational Database Management System (RDBMS) client/server environment. It can be licensed to operate on a Microsoft® SQL Server platform. The SQL Server version supports SQL Server, Standard or Enterprise Editions. It is the client's responsibility to procure all licensing for the RDBMS.

The application does not have a server component. Instead, it communicates directly with the RDBMS server through the RDBMS system client software. The application must be executed on a workstation computer running Microsoft® Windows Professional, or on an application server running Microsoft® Windows Server.

The application is supported on Microsoft® Windows™ 64-bit versions using the WoW64 execution layer. WoW64 (Windows 32-bit on Windows 64-bit) is a subsystem of the Windows operating system that is capable of running 32-bit applications and is included on all 64-bit versions of Windows.

The application is highly scalable, and it can be configured to operate in a number of different networked environments. Proper configuration will depend upon the type of network, the number of sites, the number of users.

For a traditional client/server implementation, the application software can be installed on the individual workstation PC's, or it can be housed on one or more application servers and executed from local workstations. In a thin client/server implementation, the software is installed on one or more application servers (Citrix or Terminal Services).

The database should generally be placed on a separate database server. In some cases, the database can reside on a common server with the application software. However, if the organization serves a large number of users or has multiple locations, we recommend that the database have its own server.

On-Premise Environment

The Microsoft SQL Server database must be installed on a server that is accessible to each client workstation or application server that will be executing the application. Depending on the database version, this server can be any operating system accessible to Microsoft Windows workstations and capable of housing the database. It is perfectly acceptable for the database server to be accessed both locally by client workstations and by one or more application servers.

In a single-site, Local Area Network environment serving a small to medium number of users, the typical implementation involves installing the software on the local workstations to run against a single network database server. Alternatively, to ease deployment the application can be placed on the database server or on its own file server, and executed from the local workstations. The trade-off between greater network performance and greater ease of deployment should govern which method to use. In addition, clients should utilize networking hardware that supports a minimum connection of 100 Mbps.

In a Wide Area Network environment, the software requires the use of a thin client/server technology such as Windows Terminal Services and/or Citrix®. For very large, widely dispersed networks, we recommend using Citrix, for well-documented performance, reporting and security reasons. In these types of implementations, many thin client hardware devices can be employed in lieu of more expensive workstation PC's. Clients must obtain a sufficient, secure and reliable broadband network connection that will handle the network traffic, given the total number of users on the network.

Net Health is not in the business of designing or installing networks, hardware or communications devices. The software will function correctly on any network configuration that efficiently supports Microsoft Windows applications and TCP/IP. For purposes of both network communications and database access, the application requires TCP/IP in order to accommodate wireless networking, scanning, auto-faxing and auto-emailing.

Net Health does not provide licensing for Microsoft or Citrix products. It is the responsibility of Net Health' clients to obtain proper licensing for SQL Server, Microsoft Windows and Citrix, if employed.

Technical Requirements

In addition to the standard requirements for servers, workstations and network hardware, this section describes special configuration options that apply to clients who want to make use of certain features in the software, such as scanning and image storage, electronic signature capture, automated faxing and emailing, and Adobe forms.

The following sections provide the detailed requirements and guidelines to be used in selecting hardware, networking and special add-on options.

Database Server Requirements

Assuming the software database will reside by itself on its own computer, the following guidelines apply. Special considerations are noted for those clients who elect to store images using the scanning and imaging function. The minimum required column applies to smaller, single site installations. Larger implementations should follow the recommended guidelines as a minimum.

Hardware Requirements:

1-50 Concurrent Users:

CPU	2GHz or faster (2 or more processors)
Memory	4 GB or greater

50-100 Concurrent Users:

CPU	2GHz or faster (4 or more processors)
Memory	8 GB or greater

>100 Concurrent Users:

CPU	2GHz or faster (4 or more processors)
Memory	16 GB or greater

Average Storage Requirements:

An average estimate of storage requirements is 20 GB of storage per 10,000 visits with an average of 3 scanned document images per visit.

You can also use these formulas to estimate the overall storage required per year:
(# of patient visits yearly) * (600 KB per visit) = total estimated storage per year (in KB) for visits
(# of patient visits yearly) * (# images per visit) * (160 KB per image) = total estimated storage per year (in KB) for images

You then add the resulting values together to estimate the annual database storage needs.

SAN Storage is supported for storage of MS SQL Server Database. You should refer to Microsoft SQL Server technical documentation for details.

RAID Level. Any RAID level used that is supported for storage of MS SQL Server Database. You should refer to Microsoft SQL Server Technical Documentation for details.

Backup System. Net Health requires at least a daily backup of your database. To support this, you should employ a backup system that can adequately handle the volume of data stored and fully supports Microsoft SQL Server database system that you choose. (Refer to the next section, entitled *Routine Database Backups.*)

NOTE: The software will support only the vendor supported versions of any required software.

Operating Systems Supported: Windows Server (32-bit or 64-bit)

Microsoft SQL Server Versions Supported: Microsoft SQL Server Standard or Enterprise Editions

Virtualization Support: VMWare - VSphere

Additional Required Software Components: .NET Framework 4.7.2 or greater

* For further information, please refer to *Capacity and Performance Planning* section below, as well as the current requirements published by Microsoft for your selected RDBMS.

Routine Database Backups

Net Health strongly recommends that routine backups be made of the software Database following your organization's Disaster Recovery Plan. Furthermore, it is recommended that you encrypt your database backups, especially if they are to be stored on removable media such as Tape or DVD, in order to minimize the risk of exposing Protected Health Information (PHI) in the event that your database backups are lost or stolen. Many commercially available products exist that can manage this task. The following are just a few examples. You should consult with your database administrator and security officer to determine what your needs are.

- Redgate SQL Backup Pro
  http://www.red-gate.com/products/SQL_Backup/index.htm
- Idera SQL Safe Backup

  http://www.idera.com/Products/SQL-Server/SQL-safe-backup/
- Barracuda Networks Barracuda Backup Service

  http://www.barracudanetworks.com/ns/products/backup_overview.php

At a minimum, Microsoft SQL Server also provide Secure Backup features to encrypt your backups. Please refer to the documentation provided by these providers for details on encrypting your backups.

Citrix or Terminal Services Server Requirements

The following guidelines apply to a Terminal Services or Citrix application server that will be executing the software in a thin client/server installation. The minimum required column applies to installations with ten or fewer users per server. The recommended column applies to larger installations with 20 to 25 users per server.

Hardware Requirements: (up to 25 concurrent users per-server)

CPU	2GHz or faster (2 or more processors)
Memory	4 GB or greater
Application & Temp Storage	10-20 GB estimated maximum

Operating Systems Supported: Windows Server (32-bit or 64-bit)

Citrix Server Versions Supported:

- Presentation Server for Windows Server (32-bit)
- XenApp for Windows Server (32-bit or 64-bit)

Software Required by the Application:

- Net Health Interop Components
- Adobe Reader (needed for pre-fill and print only Adobe forms)
- Adobe Acrobat (only needed for interactive Adobe forms)
- Exit Care Client (OM & UC customers only)
- SQL Native Client 11.0 and .Net Framework 4.7.2
- Virtualization Support:
- VMWare - VSphere

* Information about Citrix Presentation Server/Xenapp products can be obtained at www.citrix.com. Since these changes periodically, client should work through a local Citrix reseller.

"Fat" Client Workstation Requirements

The following requirements and recommendations apply to any workstation that will be directly executing the software, whether the software is loaded on a hard drive locally or on a server hard drive.

Hardware Requirements:

CPU	2GHz or faster (2 or more processors)
Memory	4 GB or greater
Application & Temp Storage	2-10 GB estimated maximum

Operating Systems Supported:

Software Required by the Application:

- SQL Native Client 11.0 and .Net Framework 4.7.2
- Net Health Interop Components
- Adobe Reader (needed for pre-fill and print Adobe forms)
- Adobe Acrobat Standard (needed for interactive Adobe forms)
- Exit Care Client (for OM and UC customers only)
- Topaz SigPlus Basic electronic signature software (if installing Topaz eSignature pad)

Other Requirements

To view the software optimally, the software must run on a workstation with a ***screen resolution*** of **1600 x 900 or higher**; and for optimal user experience, display scale should be set to 100%.

* Note that if this workstation is to be used for serial or USB communications with special equipment devices that are supported by the software, (scanners, audiometers, spirometers, etc.), you must make sure that the proper connections are available to support such an interface. Check with your equipment vendor for specifications.

"Thin" Client Workstations for Citrix/Term Services Implementations

Organizations employing Citrix have been able to work very successfully with the software. A Citrix client can be an Intel PC, a Wyse Winterm, an Apple computer, or a variety of inexpensive devices. Follow the guidelines supplied by Citrix Systems, Inc., for more information. Due to the complexities involved in the technologies required for scanning, any thin client device should be tested for proper functioning before purchasing in a production environment.

Hardware Requirements:

Any thin client workstation or device that can support access to a Citrix / Terminal server, as well as meet the following requirements in this section.

Operating Systems Supported: Windows Professional (32-bit or 64-bit)

Citrix Client Versions Supported (depends on Citrix Server version):

- Citrix Presentation Server Client
- Citrix XenApp Client
- Citrix Receiver

Software Required by the Application:

- .NET Framework 4.7.2. Only needed when using the Net Health Citrix or Terminal Services add-on to support Scanners, Signature Pads, Cameras, or doing Image imports.
- Net Health Citrix or RDP Client Add-On Components (the software supports Remote Access RDP versions 7.0 through 8.1. This support will only continue **for the duration of Microsoft's support of Windows 7**)
- Topaz SigPlus Basic electronic signature software (if installing Topaz eSignature pad)

When deploying with Citrix, your users can all access the application using the patented Citrix ICA client. This client is downloaded from the Citrix web site www.citrix.com, and also supplied from the software installation executable. In addition, the Citrix server can be configured to allow your users to access the application through a web browser such as Microsoft Internet Explorer.

To view the software optimally, the software must run on a workstation with a ***screen resolution*** of **1600 x 900 or higher**; and for optimal user experience, display scale should be set to 100%.

General Network and Broadband Requirements

Clients must obtain a sufficient, secure and reliable network connection that will handle all of the network traffic (including the software), given the total number of users and applications on the network. Large organizations using Citrix or Terminal Services may want to consider, for purposes of encryption and security, establishing a Virtual Private Network (VPN) tunnel for remote connections to the server(s). However, Citrix security settings pass all requirements for security encryption, regardless of whether a VPN is being employed.

The amount of network traffic, the number of simultaneous users, the number of applications being supported, and the network costs are factors that will influence this selection.
For LAN based implementations, Net Health recommends that the internal network is operating at least **100 Mbps**.

For WAN based implementations, Net Health recommends that the internal network is operating at least 100 Mbps and that each Remote location connection is at least a T1 or equivalent network connection operating at 1.5 Mbps or greater. Regardless of the type of broadband connection, you need at least a **5 Mb symmetrical connection**.

In addition, clients must obtain a reliable and secure broadband access to the Internet operating at 1.5 Mbps or greater in order to obtain program updates and access guidelines from the software. Again, regardless of the type of broadband, you need at least a 5 Mb symmetrical connection.

Virtual Computing Requirements

Many large organizations such as hospitals are electing to utilize virtualization technology, such as VMWare, in order to optimize their use of physical computer resources. The software may be run or deployed using virtual computing, as long as the virtualization technology fully supports all of the features of Windows. In a virtual environment, the computer resources provisioned to the software must be equivalent to those provided by the physical computer(s) matching the specifications outlined in this document. The software supports VMWare - VSphere or higher.

Printer Requirements

The software generates many reports, forms and graphs, and utilizes standard Windows fonts. Consequently, Net Health guarantees successful printing only on devices that support standard printing capabilities employed by Microsoft Windows and standard Windows applications. It is highly recommended that HP or compatible laser printers be employed for all heavy-duty printing. However, most Windows-supported dot matrix, inkjet and label printers can be used in situations where they are necessary and the printing load is not overly demanding for the type of device being employed.

Regardless of the type of printer, it is essential that all printers be compatible with and controllable by Microsoft Windows, and that the correct and latest Windows printer drivers be installed. The software does **not** interact directly with any printer driver. Windows handles all of the actual printing function.

In a typical provider clinic operation, the client will need to have medium duty printers in the check-in and check-out areas (these can be the same printer if appropriate), one or more heavy duty printers in the back office for billing and reporting, a prescription printer if printing prescriptions, and possibly one or two label printers if printing encounter or dispensed med labels.

Scanning and Image Capture Requirements

Net Health provides a powerful scanning and image capture function, which is licensed separately as an optional add-on feature. The software **Scanning and Imaging** function allows you to capture and retrieve both text and image based documents such as x-rays, test results, old patient charts, patient photographs and a variety of other documents. When doing so, the client can configure different document types to use resolutions appropriate to the type of document. Images can be captured directly from a scanner or digital camera, or they can be imported from an image file on disk (supported image formats include JPEG, BMP, GIF and PDF).

Clients must make sure to have plenty of disk space on the database server, along with a reliable highspeed backup system (see *Database Server Requirements* above).

In order to capture images directly from a scanner or a camera, the software requires that the image capture device fully support the Windows Image Acquisition (WIA) protocol. Net Health chose the WIA protocol over the older TWAIN protocol because of its relative

simplicity, its flexibility in supporting different kinds of devices, and its integration with the Microsoft operating systems.

As is the case with printers, the software does **not** interact directly with any scanner. Windows handles all of the actual scanning function. Therefore, you must have the appropriate Windows device driver loaded for each scanner. ***Many modern scanners and digital cameras on the market today fully support the WIA protocol, but others provide only partial support, or claim to provide support but fail to do so***. However, when choosing your equipment, be sure (1) to check ***with the manufacturer*** for its Windows (***WIA***) compatibility, and (2) ***test the model of your choice with the software*** before purchasing for production.

The software **Scanning** function requires the following for each scanning station:

- A scanner (or digital camera) that fully supports the Windows Image Acquisition protocol, and preferably is Microsoft WIA certified (see more discussion below),
- If a Wyse Winterm is being used as a thin client device, then the Microsoft Embedded version must be used.
- The .NET ("dot net") Framework 4.7.2 installed on each computer that will be executing image acquisition,
- PDF Reader, on each computer that will be either executing image acquisition or viewing scanned images from the database.

In a typical provider clinic operation, the client may want to have medium duty scanners in the check-in and check-out areas (these can be the same scanner if appropriate), and one or more heavy duty scanners in the back office for charting and/or billing document capture. The check-in scanner should be able to scan insurance cards and driver's licenses, in addition to paper. The heavy duty back-office scanner should be able to handle multiple documents, and preferably support simultaneous front and back side scanning. For this reason, a flatbed scanner is not recommended. ***In addition, for equipment involved in heavy duty document scanning, Net Health strongly recommends employing a scanner that can print the date and time stamp on the back of a document when it is scanned.***

In order to achieve a reasonable rate of performance Net Health recommends purchasing scanners that meets the following minimal ratings:

Monochrome scan rates capability of 25 pages per minute (ppm) simplex, 50 images per minute (ipm) duplex @ 200dpi.

Color scan rates capability of 30 pages per minute (ppm) simplex, 60 images per minute (ipm) duplex @ 150dpi.

If you do not adhere to these recommendations, you may not get satisfactory response times when scanning. If you intend to engage in heavy-duty scanning, such as scanning old patient charts, you should purchase a more robust scanner.

Net Health does not sell or directly support scanning equipment. Also, it has been our experience that ***many scanners do not actually perform in accordance with their published***

ratings. While we do not represent or sell scanning equipment, we have obtained sufficient feedback from our clients to ***strongly*** recommend Fujitsu scanners. At the time of this writing, the following models have received very good reviews from a number of Net Health clients:

- Fujitsu 5120c (excellent for scanning at the front desk – light to medium usage)
- Fujitsu 6130c (excellent for scanning at the front desk – light to medium usage)
- Fujitsu 5530c (heavy duty scanner designed for up to 3000 documents per day)

Scanning models change frequently. If you decide to explore other scanning models or manufacturers, be sure to contact Net Health Technical Support to consult before purchasing your scanning equipment. Net Health cannot support a scanner that is not 100% compatible with WIA. ***From our experience, Net Health strongly recommends getting a demonstration of the scanner you wish to purchase and testing it with the software before final purchase.***

PDF Forms Requirements

The software provides two types of form handling capabilities, each using Adobe PDF forms technology. Pre-fill-print (PFP) forms enable the client to have special, tailor made forms that will print at check-in, pre-filled with relevant patient information. Pre-fill-interactive (PFI) forms allow clients to view, fill out and save user-defined forms as images in the database.

Both of these types of forms rely upon version 1.7 of the Portable Document Format (PDF) technology platform pioneered by Adobe Systems Incorporated. With Adobe Acrobat Professional, clients have the ability to create PDF version 1.7 forms, the only PDF version that meets the requirements set by the International Standards Organization (ISO).
Printing PFP forms requires the following:

- The .NET (“dot net”) Framework 4.7.2 must be installed on each workstation or Citrix / Terminal server that will be printing forms from the software,
- Adobe Reader or higher.

Filling out on-line PFI forms requires the following:

- The .NET (“dot net”) Framework 4.7.2 must be installed on each workstation or Citrix / Terminal server that will be filling forms in the software,
- Adobe Acrobat Standard Edition, or higher, for each workstation or Citrix server that will be used to fill in forms interactively (clients must handle any Adobe licensing).

Creating your own user-definable forms for pre-fill-print or pre-fill-interactive entry can be accomplished through either Adobe LiveCycle Designer ES3 or Adobe LiveCycle Designer ES4 if you own licenses for one of them. If you do not have either version of Adobe LiveCycle Designer, Adobe Experience Manager Forms Designer is required.

Automated Faxing Requirements

The software **Auto-Faxing** can be accomplished using Microsoft Fax. **Microsoft Fax** is available free of charge and can be executed from any Windows workstation, and the fax server capability required for automated communications with the software is available

Windows Server. If you want to use this product, you will need to set up the fax server component to operate on a Windows application server. The fax server requires the following:

- Microsoft® Windows Server
- The .NET ("dot net") Framework 4.7.2 or higher must be installed on a Citrix /Terminal server that will be faxing from the software,
- Adobe Reader
- A Brooktrout, Intel Dialogic, Netaccess, Gammalink or other analog or digital fax board supported by Microsoft Fax (refer to Microsoft for fax board requirements),
- One or more telecom lines for sending the fax.

Any Windows client workstation that will be sending faxes must also have the .NET ("dot net") Framework 4.7.2 or higher installed.

Automated Emailing Requirements

The software **Auto-Emailing** employs a direct interaction with TCP/IP network drivers and the Windows Sockets library, which are part of the base operating system for all Windows platforms. All that is physically required is an Internet connection that is available to each workstation or application server that will need to send emails. If a dial-up connection to the Internet is being used, then the Microsoft Dial-Up Networking component must also be installed. If a direct connection to the Internet is available through your network, that connection will be used.

The software automatically employs Secure Socket Layer (SSL) technology to guarantee secured transmission (SSL is approved by HIPAA). All reports or forms that are being emailed from the software are formed into Adobe PDF attachments and are automatically encrypted, using Administrator defined encryption codes (encryption is required by HIPAA). Your clients who receive emails from the software will need the codes required for decrypting to read the email attachments.

PDF Files created by the software can also be Digitally Signed to ensure their integrity, using the SHA1 hash algorithm as implemented by the PDF 1.6 specification. To support this feature, you must supply a personal X.509 certificate. The certificate needs to be exported to a PKCS#12 Personal Information Exchange (.pfx) file and added to the software.

The software **Auto-Email** is RFC 822 and RFC 1521 MIME compliant. The email server to be used with the software, whether installed in-house or provided by an Internet Service Provider (ISP), must support SMTP or ESMTP for mail transport, and also must allow mail-relay. Likewise, the client software used to receive email must support RFC 822 and RFC 1521 formats. An Adobe Reader is required to view or print the software reports received via email attachment.

Electronic Signature Capture Requirements

The software provides the ability to capture electronic signatures with charting notes and to capture and print signatures on many other report forms. The most common way of accomplishing this is to capture one time in the user code table the signature of each provider or other user for whom documents require a signature. However, users can also sign forms “on the fly”.

Users may capture signatures with an **electronic signature device** or in some cases, they may use a **mouse, stylus**, or **touch screen**.

- Using an **Electronic Signature Capture** device:
  Because this method requires a particular type of device, Net Health has selected the state-of-the-art, patented devices developed by Topaz Systems, Inc. (see www.topazsystems.com). These devices have specifically been developed to comply with Federal standards of electronic signature capture, including the HIPAA Standard.

- **Using a mouse, stylus,** or **touch screen:**
  This feature is only available on Microsoft Windows devices with touch screen capabilities, or Microsoft Surface devices in desktop mode only.
  If one of these types of devices is present, patients (employees) may sign their opened prefill interactive forms using a mouse, stylus, or touch screen. The signature is then captured, stored, encrypted, and printed on the form.

Capacity and Performance Planning

Performance Guidelines

The software Response Time Performance Standards:

The software is designed to perform consistently with the following average response times:

- The average data-field to data-field response time not to be greater than two (2) seconds 95% of the time.
- The average screen-to-screen and tab-to-tab response time not to be greater than two and one-half (2 ½) seconds 95% of the time.
- No function greater than three (3) seconds 95% of the time.

Excluded from the above performance standards are delays due to: large queries (requiring multiple record access); any functions that require multiple inserts, deletions, or updates; Adobe forms execution; batch reports; interfaces; initial program load time; updates and/or upgrades; data backups; improper configuration of the hardware or third party software; timing related to excessive network traffic; or insufficient bandwidth.

Also excluded are certain setup functions, including but not limited to, the operation of the template builder, user and security set-up and the like, and performing a batch operation or initially loading a software module, or requests to display more than twenty (20) records per workstation simultaneously.

All response time targets are invalidated if: (1) any software other than the software is running on the server or workstation; (2) workstation and server recommended configurations outlined in the software Technical Specifications document are not followed; or (3) the number of databases, workstations and/or concurrent users exceeds those outlined in the previous section of this document.

Hardware and Networking Capacity Guidelines

The ability to ensure that the software will operate within the above response time standards is dependent upon two primary factors: (1) the number of users, and (2) the number of physical locations and network connection among locations. It has been our experience that the type of database (SQL Server) is generally not a factor in performance. Microsoft SQL Server provide comparable response times with the software.

The following are intended to provide general guidance in configuring your hardware and network equipment to operate consistently with the software response time standards.

Database Server:

Net Health has found Microsoft SQL Server to be similar in performance.

Hardware Requirements:

1-50 Concurrent Users:

CPU	2GHz or faster (2 or more processors)
Memory	4 GB or greater

50-100 Concurrent Users:

CPU	2GHz or faster (4 or more processors)
Memory	8 GB or greater

>100 Concurrent Users:

CPU	2GHz or faster (4 or more processors)
Memory	16 GB or greater

Average Storage Requirements:

An average estimate of storage requirements is 20 GB of storage per 10,000 visits with an average of 3 scanned document images per visit.

You can also use these formulas to estimate the overall storage required per year:

- (# of patient visits yearly) * (600 KB per visit) = total estimated storage per year (in KB) for visits
- (# of patient visits yearly) * (# images per visit) * (160 KB per image) = total estimated storage per year (in KB) for images
- You then add the resulting values together to estimate the annual database storage needs.

Terminal / Citrix Application Server: WAN Environment

Net Health recommends Citrix servers for WAN environments.

Hardware Requirements: (up to 25 concurrent users per-server)

CPU	2GHz or faster (2 or more processors)
Memory	8 GB or greater
Application & Temp Storage	10-20 GB estimated maximum

Technical Services, Protocols and Ports

Depending upon the configuration and licensing, the software makes use of a number of technical services and protocols. Some of these are built-in, and some are utilized only in relation to licensed interface modules.

This section is intended to provide a recap of the possible services and protocols, including associated ports and required security privileges where applicable, as a reference for System Administrators and client IT staff who are responsible for implementing and/or supporting the software application.

Wherever applicable, we have included information about how the software protects the confidentiality, integrity and reliability of data to which the service applies when communicated over an open network.

NOTE: The software supports Remote Access RDP versions 7.0 through 8.1. This support will only continue **for the duration of Microsoft's support of Windows 7.**

Overview

Function	Protocol	Port / Range	Service
Time Synchronization	NTP	UDP 123	Network Time Service
Auto-Emailing	SMTP	TCP 25 (outbound only)	Email
Clinical Guidelines Access	HTTP	TCP 80	Various Websites
Inbound Hospital Interface	HL7	TCP (1024-49151) Customer Specified	Hospital Interface Service
Outbound Hospital Interfaces (Lab, MPI, etc.)	HL7	TCP (1024-49151) Customer Specified	Proprietary Inbound Hospital Interface Services
Outbound Hospital Billing Interface	FTPS	TCP 990	Secure FTP Server (Upload)
CRL Lab Interface	FTPS	TCP 990	Secure FTP Server (Download)
LabCorp Lab Interface	HTTPS	TCP 443	Hypersend Web Services
Quest (Toxicology)	HTTPS	TCP 443	Hypersend Web Services
Quest (Clinical Lab)	HTTPS	TCP 443	Care 360 Web Services

On-Premise Environment

Audit Log Repository	UDP/IP	Any available UDP port (UDP 514 recommended)	Syslog Server
Remote Access	RDP	TCP 3389	Microsoft RDP Windows Client
Remote Access	RDP / HTTPS	TCP 3389 / TCP 443	Microsoft RDP ActiveX Client
Remote Access	ICA	TCP 1494	Citrix Windows Client
Remote Access	ICA / HTTPS	TCP 1494 / TCP 443	Citrix Web Client

Built-In Application Services

Local Area Network Access

All closed local area network operations of the application make use of direct API interaction through the Microsoft Client and Server operating system, using TCP/IP as the foundational networking protocol, in conjunction with the standard database security measures provided by Microsoft SQL Server. (Note that database security must be as configured by a qualified DBA! Net Health does not provide these services.)

Printing

All printing is controlled and addressed through the MS Windows operating system. Printers must be set up as either local or network printers through MS Windows. If applicable, proper security measures for individual devices should be followed by the Network Administrator.

These services are invoked from within the software application itself and are accessible by any valid user for whom the printer is configured through Windows. Configuration of printing devices and associated services should be done by qualified network administrator.

Scanning

All scanning is controlled and addressed through the MS Windows operating system, using the Windows Image Acquisition (WIA) protocol for image retrieval, in conjunction with Microsoft .NET (“dot net”) Framework 4. If applicable, proper security measures for individual devices should be followed by the Network Administrator. For practical reasons, scanners are generally attached locally to a controlling workstation, as opposed to being a stand-alone network device. Each application server or workstation used to control scanning must have the Net Health Interop Components installed in addition to the application software. Refer to the Technical Requirements chapter for additional details.

These services are invoked from within the software application itself and are accessible by any valid software user for whom the scanner is configured through Windows. Configuration of scanning devices and associated services should be done by qualified network administrator.

Auto-Faxing

Auto-faxing (outbound only), is controlled and addressed through the MS Windows operating system, using Microsoft Fax in addition to Microsoft .NET (“dot net”) Framework 4, and a reliable fax card on the fax server computer. Proper security measures for the fax card device should be followed by the Network Administrator. Each application server or workstation used to control faxing must have the Net Health Interop Components installed in addition to the software application software. Refer to the Technical Requirements chapter for additional details.

These services are invoked from within the software application itself and are accessible by any valid User. Use of these services requires the Windows User to be a member of the Fax

Operators Group. Configuration of these services for use by the application must be done by a Windows System Administrator or Network Administrator, using Microsoft Fax Services. Configuration of the application to uses these services must be done by a User that has System Administrator Access Rights, using the Administration module.

Auto-Emailing

Auto-emailing (outbound only), is controlled and addressed through MS Windows Sockets, using the SMTP protocol and SSL/TLS. No clinical content is permitted in the body of the email. Any reports or forms are emailed as encrypted Adobe PDF attachments, using the Adobe PDF 1.6 encryption method which utilizes the 128-bit AES (American Encryption Standard) algorithm.

PDF Files created by the software are also Digitally Signed to ensure their integrity, using the SHA1 hash algorithm as implemented by the PDF 1.6 specification. PDF Files created by the software, are created using either PDF version 1.3 or 1.4 and can be accessed using Adobe Reader version 7.0 or higher, requiring password access by the user. The strength of the password is controlled by the Security Administrator.

These services are invoked from within the software application itself and are accessible by any valid User. Configuration of these services for use by the application must be done by a User that has System Administrator Access Rights, using the Administration module.

Wide Area Network Access from Remote Locations

The software requirement for wide area network access from remote locations, whether remote offices or physician home workstations, is minimally through Microsoft Terminal Services, with FIPS SSL/TLS enabled for proper security and encryption. In addition, Citrix Presentation Server is recommended, with application publishing by a certified Citrix administrator. For network connectivity, Net Health recommends clients utilize either a non-public direct connection or a VPN.

There are numerous features of both Microsoft Terminal Services and Citrix Presentation Server, each of which has specific ports required for their use and should be configured by a certified network administrator. The following lists the ports necessary for remote access by the various client components needed to access the software in this manner.

NOTE: The software supports Remote Access RDP versions 7.0 through 8.1. This support will only continue **for the duration of Microsoft's support of Windows 7.**

- Microsoft RDP — TCP Port 3389
- Microsoft ActiveX Client — TCP Port 80, TCP Port 3389
- Citrix Windows Client — TCP Port 1494
- Citrix NFuse — TCP Port 80,
- SSL — TCP Port 443

Configuring in this manner ensures that no database access traffic takes place across a public network, and all screen shots, keystrokes, scanned images and reports are securely encrypted across the network.

Interface Services

NOTE: For On-premise clients that use the .NET solution, some data transmission will occur outside of your private network.

Hospital Interface Services

From time to time, hospital-based software clients may purchase licensing from Net Health for one or more interfaces with other hospital systems, such as patient registration, hospital laboratories or the hospital accounting system. Each of these interfaces has its own licensing fees, and additional setup or monthly fees may be required by Net Health's hosting partner to accommodate their unique resource requirements. These must be evaluated on a case-by-case basis.

It is the responsibility of Net Health Support and our hosting provider to determine technical requirements, IP addressing and ports to be used on the hosting platform. It is the responsibility of the client to configure and manage all interfaces from the hospital side, as well as pay any fees that may be required by Net Health hosting partner.

The following sections describe the general characteristics and requirements of various interfaces that must be considered by the hospital IT staff when licensed.

Inbound Hospital Interfaces

From time to time, hospital-based software clients may purchase licensing for an inbound scheduling (Classic only), patient registration, lab or other ancillary results interface from the relevant hospital IT system(s). The software implements all such interfaces as automated services on a hosted application server, employing a stand-alone TCP/IP server Hospital Interface utility with standard HL7 2.x (2.2 or greater) messaging. The Hospital Interface utility is configurable to listen on multiple TCP/IP ports, and it provides full acknowledgment and error response handling as well as a configurable error log.

The TCP ports that the Net Health Hospital Interface listens on are configured by the Net Health Support and our hosting partner. These will generally be port numbers above the list of Well-Known Ports (0 - 1023) and listed as "unassigned" in the list of Registered Ports (1024 - 49151) as listed by the Internet Assigned Numbers Authority (IANA). Net Health's hosting partner will designate the receiving system's IP address.

Optionally, users may choose to install our Real Time File Monitor module to receive files.

The client's Interface Administrator configures the sending software and interface engine to direct interface traffic to the address designated by Net Health Support and our hosting partner. All data filtering is the responsibility of the client's Interface Administrator. Most data filtering is programmed at the interface engine, although limited filtering capability is

available in the Hospital Interface utility itself. Further information is available from Net Health Technical Support.

The inbound Hospital Interface operates as a Windows Service and must be installed by Net Health Support and our hosting partner. It is the responsibility of the client to configure and manage the sending system and interface engine.

Outbound Hospital Billing Interface

Occasionally, hospital-based Practice Management clients may purchase licensing for an outbound billing charge interface to the hospital billing system. The application accomplishes this by means of creating billing batch files, using HL7 2.x (DFT) transactions. **The software typically does not directly transmit the outbound batches, but places these files in a secure location specified by Net Health Support and the hosting partner, with routine procedures established for sending the data to its final destination.**

Optionally, the billing interface function can be configured to upload billing batch files to a secure FTP site hosted by the Hospital. If the FTP site is not hosted locally on the Hospital network, the FTP server and client must be configured to use FTP/SSL to ensure secure transmission of the files.

A third option is to send billing files via a TCPIP internet connection. This would require our .NET solution and is not available with Classic.

These outbound Hospital Interfaces operate as Windows Services and must be installed by Net Health Support and our hosting partner. It is the responsibility of the client to configure and manage the receiving system and interface engine.

Other Outbound Hospital Interfaces

From time to time, hospital-based customers may purchase licensing for a real time outbound interface for purpose of sending charting notes to a clinical data repository; or exporting demographics to a Master Patient Index (MPI) system; or sending Lab or Radiology orders to a laboratory. To accomplish this, the software builds an interface queue table within the database. A special Hospital Interface utility runs as an automated service on the hosting server, employing a stand-alone TCP/IP client using standard HL7 2.x (2.2 or greater) messaging. The Hospital Interface client utility is configurable to send to specified TCP/IP ports, and it provides full acknowledgment and error response handling as well as a configurable error log. The TCP Ports used by the Hospital Interface client utility are assigned by the Hospital network administrator, in coordination with Net Health hosting partner. Typically, the utility is configured to send to the hospital interface engine.

This service will queue, send and re-send messages until confirmed delivery responses are received. Warnings are generated to alert the designated Network Administrator about

undeliverable messages. Once messages have been confirmed as received, the Interface utility flags completed transactions in the database queue table. This provides a continuing audit trail of all messages sent to all destinations.

These outbound Hospital Interfaces operate as Windows Services and must be installed by Net Health Support and our hosting partner. It is the responsibility of the client to configure and manage the receiving system and interface engine.

Inbound Commercial Lab Results Interface

The software support interfaces from a number of national clinical and drug screen laboratory systems, including CRL, LabCorp, Quest, MedTox and others. All such interfaces utilize HL7 2.x (2.2 and higher) messaging. In all cases to date, data is received by means of data files that must be downloaded into a secure location on the local network utilizing the favored, certified mechanism provided by each individual laboratory for the client customer, (only after successful customer testing and certification by the laboratory for that customer).

Each laboratory utilizes its own means of providing secure transfer of lab result set files. Following is brief overview of the security mechanisms used by a representative sample of lab interfaces we support.

Clinical Reference Laboratory (CRL)

- Requires the use of a secure FTP client capable of connecting to the CRL FTP Server using FTPS (FTP over SSL) protocol

Laboratory Corporation of America (LabCorp)

- Requires the use of the HyperSend web-based service which uses HTTPS (HTTP over SSL) for secure communications and the MD5 encryption algorithm for password authentication

Quest Diagnostics for Toxicology

- Requires the use of the HyperSend web-based service which uses HTTPS (HTTP over SSL) for secure communications and the MD5 encryption algorithm for password authentication

Quest Diagnostics for Clinical Results

- Uses a Care360 Certified Interface which utilizes web services based technology that communicates via XML messages using the SOAP messaging protocol over HTTPS (HTTP over SSL) for secure communications.

The software then provides a utility for importing and subsequently deleting these lab result files. Importing of Lab Result Set files into the software must be done by a user who has "Information Systems" Access Rights, using the Net Health Importing & Exporting Utility. It is the responsibility of the client System Administrator to establish the procedures to ensure prompt, secure and reliable receipt of all such result sets.

Outbound e-Billing

Practice Management supports interfaces to a number of e-Billing intermediaries or clearinghouses, including WebMD, Gateway, P2P Link, and Office Ally. All such interfaces utilize either the HIPAA compliant ANSI 837 format or the HCFA National Standard Format (NSF). In all cases to date, electronic claims are submitted by means of data files that are placed by the application into a local disk file and then subsequently uploaded by authorized client personnel to an e-Billing clearinghouse, utilizing the favored, certified mechanism provided by each individual clearinghouse to the client customer, (only after successful customer testing and certification by the clearinghouse for that customer). Each of these clearinghouses provides advanced security measures for ensuring compliance with HIPAA Privacy and Security standards.

The creation of e-Billing Batch files must be done by a User that has Billing Module Access with the Invoice Posting Permission. Configuration of Billing Accounts for e-Billing must be done by a User that has Billing Module Access with Full Access to setup Payers.

After creating an e-Billing batch file, the client user is responsible for uploading to the clearinghouse website, using HTTPS (HTTP over SSL) or FTPS (FTP over SSL) for secure communications, depending on the methodology applicable to that entity.

ePrescribing

The software has been certified for e-Prescribing by the SureScripts e-Prescribing Network. Communication between the e-Prescribing Service and the e-Prescribing Gateway is handled by XML Web Services over HTTPS (HTTP over SSL) for secure communications. IP filtering is also used to prevent connection attempts from IP addresses that have not been configured by Net Health for connection to the e-Prescribing Gateway.

Communication between the e-Prescribing Gateway and the SureScripts e-Prescribing Network is handled by XML Web Services over HTTPS (HTTP over SSL) for secure communications. IP filtering is also used to prevent connection attempts from IP addresses that have not been configured by SureScripts for connection to the SureScripts e-Prescribing Network.

The e-Prescribing Interface operates as a Windows Service and must be installed and configured by a Windows User that is a member of the Administrators Group. The service process runs under the Network Service Built-in account. Since this service functions by retrieving data directly from the software's database, no special configuration settings are required for use by the client application.

Centralized Audit Record Repository

The software supports auditing to a centralized Audit Record Repository using the Audit Trail and Node Authentication (ATNA) Integration Profile published by Integrating the Healthcare Enterprise (IHE) which establishes security measures which, together with the Security Policy and Procedures, provide patient information confidentiality, data integrity and user accountability.

The software generates audit records for system events that it mediates and stores them in the software's database. When enabled to log audit messages to a centralized audit record repository, the software will create Audit Log XML Messages that meet the **RFC3881 - Security Audit and Access Accountability Message XML** specification and transmit them to a Syslog Server using the **RFC5426 - Transmission of Syslog Messages over UDP** protocol standard which utilizes the UDP/IP transport protocol.

Net Health recommends using the well-known UDP port 514, but can be configured to send Audit Log messages using any UDP port used by your Syslog Server.

Special Technical Considerations

Use of Antivirus, Malware, and Intrusion Detection Products

Net Health highly recommends the use of Third-Party software for anti-virus, intrusion detection, and malware eradication, and it is the responsibility of the customer to install, maintain, and support such products. In addition, Net Health highly recommends that regular updates to the operating system (service packs, security patches, and hot fixes) be performed to maintain security and stability of the environment on which the software is operating.

Net Health does not provide or directly support any specific products that clients may wish to use for antivirus, malware, and intrusion detection. It has been our experience that the most common third-party software products are compatible with the software. At this time, there are no known issues regarding the use of anti-virus, intrusion detection, malware eradication, or host-based firewalls with the software.
However, if the use of 3rd Party software for anti-virus, intrusion detection, or malware eradication causes performance degradation of the software, Net Health recommends that the 3rd Party software be configured to exclude automatic scanning of the application and configuration files. Additionally, the scanning of all servers and workstations should be scheduled during off-peak usage times and exclude the scanning of software's databases.

Devices Currently Integrated for On-Premise Deployment

Note: New device integration is handled by request and is considered custom development. This work will be prioritized against other work already in queue.

Direct Connect (serial or USB) is not supported in Citrix environments.
All interfaces are capable of serial port communications except where noted.

Audiometers

- AMBCO 2500
- Benson CCA-200- **File Import Only**
- Hear Trak (Recommended) – **File Import Only**
- Maico MA728M - Uses MA800 format
- Maico MA800
- MicroLab/Earscan
- MicroLab/ML-AM - Uses MicroLab/Earscan format
- Micro Audiometrics Earscan 3
- Monitor MI-5000B
- Monitor MI-6000 - Configure as MI-5000B
- Monitor MI-7000 - Uses RA500 format
- Monitor MI-7000 S - Uses MI-5000B format
- Monitor MI-7000 TR - Uses RA500 format
- Tremetrics HT-Wizard - Uses RA500 format- **Direct Connection Only**
- Tremetrics RA300 - Uses RA500 format- **Direct Connection Only**
- Tremetrics RA400- **Direct Connection Only**
- Tremetrics RA500- **Direct Connection Only**
- Tremetrics RA650 - Uses RA500 format- **Direct Connection Only**

Spirometers

- Collins Eagle II
- NDD – **File Import only, using EasyOne Connect software.** Includes following devices:
- EasyOne Plus
- EasyOn PC
- EasyOne Air
- EasyOne Pro V05
- EasyOne Pro Lab V05

- Medgraphics CPF-S/D – **File Import Only**
- OHD KOKO Pneumo Std – **File Import Only**
- OHD KOKO Pneumotach - Only pre-test result is imported

- Spirometrics PC Flow Plus - Configure as and uses Spirometrics 3350 format
- Spirotech S400
- Spirotech S401 - Configure as Spirotech S400
- WelchAllyn Spiroperfect - **XML File Import Only** from CardioPerfect software
- WelchAllyn Cardioperfect PCR100 AHA w/interp (EKG/Spirometer combo) - Configure as WelchAllyn Spiroperfect and only imports Spirometer readings. Also allows PFT and ECG PDFs to be attached to Medical Activity.

MISC.

WelchAllyn Connect Vital Signs Monitor - Model CVSM6300 – **Direct Connection Only**

Notes

- Terminology
  - Direct Connect or Transfer - Receives data straight from the device and is brought in on the Audiometry / Spirometry medical activity, usually using a serial or USB connection. **This is not currently supported through Citrix.**
  - Import - A TXT file that contains one patient and is brought in on the Audiometry / Spirometry medical activity or in the module "FILEIOP"
  - Batch - A TXT file that contains multiple patients and is brought in using the module "FILEIOP"
- Other devices may be imported but their files **must** be in the format specified in the Audiogram or Spirogram Bridge File Layouts (available through Client Services). They may be imported through:
  - Audiograms or Spirograms buttons in the module "FILEIOP" and selecting a device whose Model is set to "Other"
  - An Audiometry / Spirometry medical activity and selecting a device whose Model is set to "Other"

Communications

The following requirements ensure your organization receives important communications such as system-generated emails for account setup and maintenance as well as product updates.

- Spam filter settings to allow emails from the domain nethealth.com
- Mail server settings to allow 13.111.2.130

Portal Server Specifications minimum requirements

Server

IIS Version: 7
.Net Framework: 4.7.2 (required for Employer / Manager portal 1.8.0 and higher; required for Patient / Employee portal 1.7.4 and higher)
Windows Version: Server Windows 2012 R2, 2016, or 2019
Ram: 8 GB
Type: 32 bit (x86) (64 Bit is acceptable.)
Processor: Xeon 1.6GHz Dual Core
http://ark.intel.com/products/28030/Intel-Xeon-Processor-E5310-8M-Cache-1_60-GHz-1066-MHz-FSB

Databases

Portals: SQL Server 2012 R2, 2016, or 2019 (10.50.1600 – RTM)
Employee Health and Occupational Medicine: SQL Server 2012 R2, 2016, or 2019 (10.50.1600 – RTM)
(http://sqlserverbuilds.blogspot.com/)

*Connection to an E-mail server will also be required
Adobe Acrobat must be running on the software server

Net Health Mobile Immunization Tracking minimum requirements

- Internet Connectivity
- Mobile Devices supported:
  - Android Device
    - Eight (8) inches or larger
    - Version 8.0 or later
    - Internet Bowser: Chrome only
  - iPad
    - IOS version IOS 13 or later
    - Internet Browser: Safari only
  - iPad mini,
    - IOS version IOS 13 or later
    - Internet Browser: Safari only
- Personal Computers (PC),
  - Windows 10
  - Internet Browser: Microsoft Edge (Chromium), Chrome
- Devices must have a minimum five (5) megapixel camera
- Supported Bar Code Formats
  - EAN-8
  - EAN-13
  - Code 39
  - Code 128
  - ITF
  - RSS-14
  - OR Code
  - Data Matrix

NOTE: **The Mobile Immunization tracking feature can support UP TO 75,000 employees per event.**

Net Health Business Insights for Employee Health minimum requirements

- Internet Connectivity
- Device: Personal Computers (PC),
- Operating Systems: Windows 10 or higher
- Internet Browser: Chrome, Firefox, IE11, and IE Edge
- Minimum version of the software is 11.1.3

NOTE: Browser *Site Setting*s should *allow* pop-ups.

Net Health e-Rx Service server minimum requirements

- .Net 4.7.2 Framework or higher
- .Net 5.0 Desktop Runtime or higher
- EHOM Release 11.6.0 or higher