Employee Health and Occupational Medicine
Technical Specifications
Hosted Clients
Revised June, 2022

Table of Contents

Technical Requirements for a Net Health Hosted Service

This document provides the requirements and recommendations to guide the client Information Systems or IT staff when implementing the software using an external platform that is hosted by Net Health's hosting partner, Expedient.

Operating the software as a hosted service, equivalently referred to as an ***ASP*** (Application Service Provider), ***SaaS*** (Software as a Service) or ***Cloud*** computing service, means that the database and actual software programs are all located remotely in a secure, reliable data center, and that all of the server hardware and application software services are provided by the data center and Net Health staff. This includes the software implementation, installation of upgrades and updates, backup and recovery services, and the procurement of the hardware for housing the database and application program files.

In a hosted operation, the software customer is responsible for procuring, installing, and maintaining the workstation hardware (desktops, laptops and possibly a local fax server), networking equipment (routers, etc.), and other devices (printers, scanners, etc.) that are to be located at the client site, as well as establishing the network bandwidth and Internet service for communicating with the hosted application. This will generally save a client at least 80% of the cost of hardware and professional IT services. The client still owns the data contained in the database and remains responsible for all of its content.

The guidelines in this document not only address the technical requirements for a client to successfully use the software, but also outline additional options that are required to support special functions such as electronic signatures, Scanning, Auto-Faxing and Auto-Emailing, as well as information about wireless networking with Tablet PC's for charting in the software. The specifications for workstations and laptops in this document are intended to serve as guidelines only. Individual workstation requirements may vary from these estimates on a case-by-case basis, depending upon other software implemented on the same workstations and local network (such as, for example, Microsoft Office). Likewise, bandwidth requirements will depend upon the number of users, volume of transactions, type of network, and other software implemented on the same workstations and local network. Final decisions about hardware and networking technologies should be made by a qualified networking consultant or other qualified IT personnel.

General Overview

The software is a 32-bit Microsoft® Windows™ based applications, designed to operate through Citrix in a hosted environment. The software program itself is executed on server hardware that is fully housed at the Expedient data centers. The only hardware needed on the local network is the workstations (desktops, laptops, notebooks), devices (printers, scanners, signature capture tablets), network routers for accessing the Internet, and possibly a local fax server.

In addition to procuring, installing, and maintaining the local network, the client is responsible for purchasing the licensing for and maintaining the local network and workstation operating systems. Typically, this will be using Microsoft Windows. However, any operating system that supports access through the Citrix Internet client will work.

Note that Net Health does not provide either hardware or licensing for Microsoft or other locally desired software or hardware products. It is the responsibility of the client to obtain proper licensing for these. However, Net Health's hosting services include all licensing for the database (Microsoft SQL Server), the Microsoft server operating systems and the use of Citrix at the data centers. These are included in the hosting fees, based upon the number of users.

Specific Configuration Requirements and Options

In addition to the standard requirements for local workstations and network hardware, which are described in more detail in the remainder of this document, there are special configuration options that apply to clients who want to make use of certain features such as scanning and image capture, electronic signature capture, automated faxing and emailing, user-defined pre-fill-print (PFP) or pre-fill-interactive (PFI) forms, tablet PC's for the sotware charting and hospital or laboratory interfaces. These topics are discussed separately below under their own topic headings. The following sections provide the detailed requirements and guidelines to be used in selecting hardware, networking, and special add-on options.

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

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

Additional Required Software Components: .NET Framework 4.7.2 or greater

Workstation PCs and Laptops for Hosted Implementations

Because all of the processing and data storage are handled at the hosting data center, organizations licensing the software as an ASP can utilize any type of workstation or laptop that can access the Internet and support the Citrix client / receiver. This can be a desktop PC, a laptop or notebook, a Wyse Winterm, or a variety of inexpensive devices. Follow the guidelines supplied by Citrix Systems, Inc., for more information. (As noted below, certain special requirements apply to computers that are to be connected to scanners or for faxing.

To run the software, the workstation device must have broadband access to the Internet through your Internet Service Provider and be able to execute the Citrix client / receiver in conjunction with a web browser. This Citrix client / receiver is downloaded free of charge from the Citrix web site www.citrix.com.

If you plan to use a workstation for other applications, such as Microsoft Office, you should make sure your workstation has sufficient memory and disk storage capacity to support use of those applications. Also, make sure your workstation has a fast network (NIC) or wireless access that supports at least 100 Mbps.

To view 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%.

Users who will be using scanning devices or capturing electronic signatures through Citrix client / receiver workstations will need an additional add-on provided by Net Health, which will allow them to utilize these devices in the application.

General Network and Communications Requirements

Net Health is not in the business of designing or installing networks, hardware, or communications devices.

Within your Local Area Network (LAN) environment, clients should utilize networking switches or routers that support a minimum connection of 100 Mbps.

To connect to the hosted platform, clients must obtain a sufficient, secure, and reliable broadband Internet connection that will handle all of the network traffic, given the total number of users and applications on the network. Any firewalls will need to be configured to support Citrix connections.

Charting Tablet Requirements

The software charting is designed to make maximum use of the special features of Tablet PCs in a wireless network environment. When operating on a Tablet, the EMR fully supports Microsoft's built-in pen and voice technologies for data input, as well as all of the latest wireless technologies for networking. For information about pen and voice technologies, you should refer directly to Microsoft.
Following are the requirements and recommendations for configuring a Tablet for use with the software. Note that these are generally the standard minimum features of all reputable name-brand Tablets.

- A "convertible" style Tablet with an Intel Pentium M Processor, 1 GHz or higher. Convertible tablets come with a swivel-attached built-in keyboard that allows the user to type, in addition to using pen and voice technologies. A keyboard is required at the very least for user code and password logins, and many physicians may prefer to type in other situations. Built-in keyboards are preferable to separate wireless keyboards.
- Integrated wireless technology (Centrino Tablet recommended).
- Microsoft Windows Tablet (latest service pack recommended).
- Pen stylus (with additional spare) for pen-based entry and built-in microphone if voice entry is desired.

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 the sophisticated printing capabilities employed by Microsoft Windows and standard Windows applications. It is highly recommended that HP or compatible laser printers be employed for all printing. However, Windows-supported dot matrix, Desk Jet 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).

In order to capture images directly from a scanner or a camera, the application requires that the device be compatible with Windows and 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 support from Microsoft, and our own proprietary internal technology for managing the scanning process across the Internet through Citrix.

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 **Scanning** function requires the following:

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

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.***

Special Net Health Forms Requirements

Net Health provides two types of form handling capabilities. 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.

Printing PFP forms with the hosted software does not require any special licensing or setup on the part of the client. However, filling out on-line PFI forms requires network licensing by the client for Adobe Acrobat® Standard or Pro edition for **all** users. If you will be using an Adobe Acrobat Standard license, you must purchase it directly through Net Health.

Creating your own user-definable forms for pre-fill-print or pre-fill-interactive entry requires Adobe LiveCycle Designer ES3 or Adobe LiveCycle Designer ES4.

Automated Faxing Requirements

Net Health provides the ability for clients to send faxes directly from the software to their client customers. Because the hosting data center cannot provide direct telephone lines for such a service, clients must arrange to utilize one of two methods for doing this: (1) faxing through a local fax server that is set up on the client's local area network and is visible to every workstation user who will be sending a fax, or (2) contracting with an independent Internet faxing service.

The first option requires setting up on your local network a physical fax server, which can be either a stand-alone new server or an existing server that has a fax card and a connection to one or more telephone lines. The second option requires establishing a pre-paid business account with Interfax, a national Internet faxing service with which the software is integrated.

Auto-Faxing with a Local Fax Server

Net Health **Auto-Fax** can be accomplished using Microsoft Fax from a local network fax server through your own telephone lines. When using this method, all faxes from the Net Health software must be directed through Citrix to your local server, and the fax server will send them through your telephone lines. **Microsoft Fax** is a software product available free of charge that can be executed from a Windows Server. If you want to use this product, you will need to set up the fax server component to operate on a server on your local area network that is available to all workstations accessing the software application that will be utilizing the auto-faxing capability. 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.

Any client workstation that will be sending faxes must also have the Windows 10 or Windows 7 operating system installed as well as the .NET ("dot net") Framework 4 installed. Local Microsoft Faxing cannot be initiated using Apple workstations or Microsoft workstations using earlier versions of Windows.

Auto-Faxing with an Internet Fax Service

Interfax US, Inc. is an independent Internet faxing service with which Net Health has fully integrated application. It requires no special hardware or operating system to be used on the client workstation. In order to fax using this service, clients must make business arrangements directly with the Interfax service, which operates on a pre-paid basis. Information and pricing can be obtained at www.interfax.net.

Automated Emailing Requirements

Net Health **Auto-Email** employs a direct interaction with the TCP/IP network, which is all part of the base operating system set up by the software hosting provider and requires no special licensing on the part of the client.

The application 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 these emails will need the codes required for decrypting in order to read the email attachments.

PDF Files created by the software may 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 application by Net Health support personnel.

Net Health **Auto-Email** is RFC 822 and RFC 1521 MIME compliant. Likewise, the software used by the ultimate recipients to receive email at the other end must support RFC 822 and RFC 1521 formats, and the Adobe Reader is required for recipients to view or print reports received via email attachment.

Electronic Signature Capture Requirements

Net Health 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.

Interface Services

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 software

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

The software 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 user that has Billing Module Access with the Invoice Posting Permission. Configuration of Billing Accounts for e-Billing must be done by 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 the software 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 software 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.

Equipment Integration Available for Use Within Hosted (Citrix) Environments

Direct Connect (serial or USB) is not supported.

Audiometers

- AMBCO 2500
- Benson CCA-200
- Hear Trak
- 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 (Using HearCon Software, File Import Only)
- Tremetrics RA300 (Using HearCon Software, File Import Only)
- Tremetrics RA400 (Using HearCon Software, File Import Only)
- Tremetrics RA500 (Using HearCon Software, File Import Only)
- Tremetrics RA650 (Using HearCon Software, File Import 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
- OHD KOKO Pneumo Std
- 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.

Notes

- Terminology
  - Import - A TXT file that contains one patient and is brought in on the Audiometry / Spirometry medical activity or in the software module "FILEIOP"
  - Batch - A TXT file that contains multiple patients and is brought in using the software 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 software 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
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 Employee Health and Occupational medicine software is 11.1.3

NOTE: Browser Site Settings should allow pop-ups.

Net Health CITRIX Security Protocol

1. Hosted clients need to register for the CITRIX Self-Serve portal at https://selfservice.nethealthapps.com.
2. The initial logon ID and temporary password are provided by the Project Manager. When customers are first implemented, the Project Manager will send registration documentation to the client for them to register an Administrator Account user.
3. Additional client Administrator Account users may be created by working with the EHOM Support team. Clients may contact the EHOM Support team at ehoccmed-support@nethealth.com. Information will be provided to the client.
4. Clients should log into the portal using their assigned login ID and temporary password. They may access the Account Settings at the top right of the portal window by clicking the "Gear Box" icon. At this point, clients may change their temporary password into a unique, permanent one.
5. To change passwords, clients may follow the same process as step #4 above.
6. Forgotten login credentials (ID and password) may be changed through the CITRIX Self-Serve portal. A link is provided on the home page of the portal.
7. Citrix Security parameters and rules:
    a. Password length and required characters include 12 characters, with 3 unique characters:
        i. 1 Uppercase character.
        ii. 1 Lowercase character.
        iii. 1 Numeric or special character.
    b. Account lock for failed attempts:
        i. After 3 invalid login attempts, the account will be locked.
        ii. The lockout remains in effect for 30 minutes.
    c. Session time-outs:
        i. After 2 hours of inactivity, the session is disconnected.
        ii. After another 8 hours, the session is completely logged off.
    d. Password expirations
        i. Every 90 days, user passwords will expire.
        ii. The system will remember 24 passwords and restrict their reuse.

Net Health Multi-Factor Authentication (MFA) minimum requirements and setup procedures

Net Health enables MFA exclusively through DUO. In order to begin the process, customers will need to establish an account with DUO.

Once the customer has an account, the following procedures will complete the installation:

1. The customer's DUO Administrator will need to add the Citrix Netscaler APP to implement protection. This can be found by selecting "Protect an Application" within the portal.

2. The customer needs to submit a support ticket requesting DUO installation to the following email address: ehoccmed-support@nethealth.com
   They will need to provide the following information:
   - Duo Administrator name, contact number, and E-mail address
   - Integration Key
   - Secret Key
   - API hostname
   - Which users they would like configured for initial deployment

3. Net Health Support will create an IT request ticket.

4. The Net Health IT team will add the customer DUO-keys to our authentication service and complete the installation.

5. Net Health Support team will be notified once the It ticket is completed. At that point, they will contact the customer to coordinate a cutover date. Finally, Net Health will confirm all users have been added and the process is working correctly.

Once Multi-Factor Authentication is enabled, customers are expected to contact Duo's support network in the event of any issues. The responsibility of ongoing support resides with Duo, the Multi Factor Authentication vendor, not Net Health.

Net Health Single Sign-On (SSO) minimum requirements and setup procedures

Net Health enables SSO through two specific vendors:

- Azure and Federation Authentication Services (FAS)
- Okta and Federation Authentication Services (FAS)

Once the customer decides they want to integrate SSO, their Account Sales representative will need to submit a support ticket requesting installation to the following email address: ClientSalesAE@nethealth.com

Depending upon which vendor is selected to implement SSO, there are Customer instructions available through the EHOM Help files in the Resource Center topic under the following names:

- Net Health EHOM SSO Azure
- Net Health EHOM SSO okta

Azure procedures and requirements:

1. Customers utilizing SSO will be provided a unique URL designated by Net Health.
2. Customers will then use this URL for the Citrix ADC SAML Connector and for Azure AD SSO configuration on the Single Sign-on SAML configuration.
3. Customers will provide a user list including the following information to EHOM Support.
   - Full Name First and Last
   - Email address
4. The customer's Azure administrator will provide specific information from the Azure Admin Console located by taking the following steps:
   a) Azure Portal
   b) Azure Active Directory
   c) Enterprise Applications
   d) Citrix ADC SAML Connector for Azure AD (Customer may label differently)
   e) Select the Single Sign-On Tab (ensure SSO with SAML is in use)
      - From SAML Signing Certificate, provide the following information:
        - Download Certificate (Base64)
      - From Set up Citrix ADC SAML Connector for Azure AD, provide the following information:
        - Login URL
        - Azure AD Identifier
        - Logout URL
        - Modify Unique User Identifier to EHOM user login that was provided by Net Health.
          - i.e. In our Proof of Concept Opened attribute editor of the user account for the internal environment and assigned extensionAttribute4 = username

*The username will be provided by Net health, **this is necessary**, so the user is properly matched up in our domain.

f) Customers will provide the EHOM user list to Net Health along with the above information for SAML Connector and certificate.
g) Net Health will then complete EHOM user assignments within their systems and return user assignments to the customer.
h) The Customer's Azure administrator will then complete the username assignments on their end.

The Authentication Process

A brief non-technical outline of how a user accesses Net Health infrastructure using their company credentials.
Citrix Netscaler communicates with Azure Citrix Gateway integration. FAS issues certs to users accessing the environment.

- User accesses custom Single Sign-On (SSO) URL.
  - Netscaler identifies traffic and directs users to Azure portal.
  - Azure will authenticate user against Customer Active Directory.
  - Azure returns with an assigned username to be used and a validated token for the user session.
- SAML token passes authentication through Netscaler.
  - Storefront issues a virtual smart card user certificate for user to access environment.
  - Certificate is assigned to the username provided by Azure.
- After authentication user is presented with applications
  - There's a setting within EHOM to enable single sign-on that must be enabled.
  - Azure username must match up with Active Directory username.

Okta procedures and requirements:

1. Customers utilizing SSO will be provided a unique URL designated by Net Health.
2. Customer will then use this URL for the Okta application configuration on the General Settings page. (For information on okta: https://www.okta.com/)
3. The customer's Okta administrator will provide specific information from the Okta Admin Console located by taking the following steps:
    a) Okta Admin Console
    b) Applications
    c) EHOM Gateway (Customer may label differently)
    d) Select the Sign-On tab, (ensure SAML 2.0 is in use)
    e) Click on 'View Setup Instructions' and provide the following information:
        - X.509 Certificate Link
        - Redirect URL
        - Single Logout URL
        - Issuer Name
4. Customers will provide the EHOM user list to Net Health along with the above info for SAML Config and certificate.
5. Net Health will then complete EHOM user assignments within their systems and return user assignments to the Customer.
6. The Customers Okta administrator will then complete the username assignments on their end.

The Authentication Process

A brief non-technical outline of how a user accesses Net Health infrastructure using their company credentials.
Citrix Netscaler communicates with Okta Citrix Gateway integration. FAS issues certs to users accessing the environment.

- User accesses custom Single Sign-On (SSO) URL.
    - Netscaler identifies traffic and directs users to Okta portal.
    - Okta will authenticate user against Customer Active Directory.
    - Okta returns with an assigned username to be used and a validated token for the user session.
- SAML token passes authentication through Netscaler.
    - Storefront issues a virtual smart card user certificate for user to access environment.
    - Certificate is assigned to the username provided by Okta.
- After authentication user is presented with applications.
    - There's a setting within EHOM to enable single sign-on that must be enabled.
    - Okta username must match up with Active Directory username.

Okta integration with DUO

Okta may perform LDAP authentication and DUO all before being handed back to Net Health systems and applications are presented. This configuration should be controlled entirely by the customer.

Once Single Sign-On (SSO) is enabled, clients are expected to contact either Okta or Azure (their selected vendor) support network in the event of any issues. The responsibility of ongoing support resides with either Okta or Azure as the SSO vendors, not Net Health.