XDR Overview & Tasks

Revised 1 JUN 2020 ksb

Obtain/Identify Domain

TASKS:

- ✓ DIVA process
  - – Also necessary when retention of a direct domain (migration)

DELIVERABLES:

- ✓ Completion of the DIVA returned securely to CliniSync
- ✓ Please keep CliniSync informed of any issues or risks

NEXT STEP:

- ✓ XDR Integration Request Form

The following Obtain/Identify Domain is just for your information

Obtain/Identify Domain

ATTACHMENT:	DirectTrust Identity Proofing Form for Sub-domain
DUE DATE:	ASAP from Date Sent
WHAT IS DUE:	Completed and Notarized form

To begin an XDR Integration with the CliniSync HISP, we will need to create a new domain address for Direct messages. While it looks similar to an email address, this type of address will only work with applications that use the Direct protocols. Due to this, the form that is attached will assist your organization in the creation of this address.

Ex.)

Hospital Name:	Samaritan Regional Hospital
Domain Required:	.medicity.net
Sub-domain Examples:	Samaritan; SamaritanRegional; SRH
New Domain Address:	@SAMARITAN.medicity.net

Obtain/Identify Domain

- Please note that your organization's choice of name will be inserted in between the @ and .medicity.net.
- There can be no additional periods or other punctuation and there can be no spaces.
- Please add your choice into the 'Requested Domain Address' field on the attached form.
- In order to add this new domain to our network we (on your behalf) are required to request a Direct compliant digital certificate through our technology partner Medicity and receive it through DigiCert, a trusted Certificate Authority (CA).
- Please complete the form per the instructions included. Be sure to complete the identity verification thoroughly, any missing fields or incorrect values will cause this form to be sent back and redone.
- *After the person chosen for the identity proofing has added their information, please have a notary complete their section, sign and stamp*.

Once complete, please scan and send this document back to me only.

Obtain/Identify Domain

As mentioned on the previous slide - once complete, the document is returned to CliniSync.

Direct-Compliant Certificates

HealthCatalyst
ignite outcomes improvement

The attached form must be completed, signed, and returned to Health Catalyst Interoperability (HCI) before we can obtain a Direct-compliant digital certificate ("Direct Certificate") on behalf of your organization from DigiCert, Inc. Direct Certificates are used to securely transmit health care information between providers. Any failure to follow the instructions contained herein may result in a delay of the Direct Certificate's issuance.

The attached form contains provisions that are applicable to you personally (as indicated in language referring to "you" or "your"), as well as provisions that apply to your organization (as indicated in language using the capitalized term "Organization"). You must sign the attached form in your personal capacity, indicating your personal agreement to the provisions applicable to "you" or "your." An authorized representative of your Organization must also sign the attached form, on behalf of your Organization.

By signing the Identity Verification, you are also agreeing to the provisions of attached authorization for Direct Certificates applicable to "you" or "your". This authorization, together with your Organization's execution of the attached form, gives HCI permission to request and use Direct Certificates in your Organization's name. HCI will use the Direct Certificates to transfer health care information to your organization in accordance with the Direct Protocol.

After the form is completed, you, a Notary (or Trusted Agent) must send a copy (pdf) of the document (authorization and ID document pages) to HCI at Hispregistration@healthcatalyst.com.

Project Initiation

TASKS:

- ✓ Completion of the XDR Integration Request Form, provided by CliniSync
  - Corresponding email will provide an overview of the form and related activities
- ✓ The XDR Integration Request Form provides essential details such as the configuration process, endpoints/public keys, etc.
- ✓ Receipt of the completed XDR Integration Request Form initiates the process with Health Catalyst/Medicity
- ✓ Details of the Form are on the Configuration slides following

DELIVERABLES:

- ✓ Return completed form to CliniSync
- ✓ Communicate to CliniSync
  - Inbound Test and Prod?
  - Outbound Test and Prod?

NEXT STEP

- ✓ Configuration

Project Initiation

ATTACHMENT: XDR Integration Request Form

DUE DATE: ASAP from Date Sent

WHAT IS DUE: Completed Request Form

The request form will:

- be used by Medicity to establish your integration request
- provide the information essential to setting up your endpoint
- request information regarding your EHR's server and where your Direct or XDR service is located
- ask for key points of contact, which will also be the first addresses, in addition to your organizational address, that will be provisioned.

I want to call out specifically the HISP Admin point of contact.

This will be the person who has complete organizational access to your domain, will be able to provision new users/addresses and have access to audit reports.

Project Initiation

Example XDR Sender URLs – Hospital Name = Samaritan Regional Hospital (SRH)

- **Meditech Magic:**
  https://SRHdirect.samaritanregional.com:20000
- **Meditech 6.07:**
  https://SRH-BG09.samaritanregional.com:443/services/SRH/SRHLIVEN/SRHLIVEN/direct
- **Epic:**
  https://ceprod.samaritanregional.com/InterconnectPRD/wcf/epic.community.hie/ProvideAndRegister.svc/mtom

You will also be asked to provide the public key from a security certificate that is installed on your server. This can be a purchased or self-signed certificate, but it must have an expiration date no earlier than 10 years from the date of implementation.

Please provide the public key as a zip file and include it as an attachment with the completed form.

Once received, the form will be submitted by to Medicity to request build.

Upon confirmation your endpoint is created, I will send you an email with your test address, a testing endpoint and guidelines for issue documentation.

Configuration

TASKS:

- ✓ Install HCI/Medicity's Public Key (inbounds)
- ✓ Apply configurations on your server/firewall to prepare for inbound and outbound activity
- ✓ Whitelist IPs
- ✓ CliniSync will provide an email containing configuration details and related activities

DELIVERABLES:

- ✓ Keep CliniSync posted on your progress and relay any issues
- ✓ Provide your endpoints for inbounds
- ✓ Provide your Public Key / Certificate for outbounds (wildcard)

NEXT STEP:

- ✓ Testing

Configuration

Medicity Direct XDR Connection Request Form

- This form is to be used by Medicity customers who already have a Medicity HISP.
- The purpose of this document is to gather information to initiate an XDR-to-HISP DIRECT connection from a non-Medicity source.
- In this document, *Customer* is the Administrator of the HISP and the *Client* is the one requesting the XDR\EHR connection.

Configuration

Medicity XDR Configuration process

- ✓ Medicity will process the request in 2 business days of receipt of the XDR connection request form.
- ✓ Once processed, Medicity will email the assigned ticket number to the Medicity customer contact for tracking purposes.
- ✓ Medicity will send the following to the remote XDR client business and technical contacts:
  - Medicity's XDR endpoint - https://xdr.medicity.net:20000/

    (For information only the IP address = 66.97.135.77)
  - Medicity's "Public Key" certificate in a zip file used for authenticating Medicity to the client's XDR endpoint

Note: Medicity Public Key is the Medicity.XDR.Client.cer. file

Configuration

Endpoints and Public Keys

Medicity requires client certificate authentication. This provides Medicity the ability to trust the client's endpoint. The certificate can be self-signed.

Note: Windows provides a MakeCert utility

a. For a <"CLIENT\EHR VENDOR"> to send an XDR to Medicity:

- In exchange for the Medicity's endpoint, the <"CLIENT\EHR VENDOR"> will send <"CLIENT\EHR VENDOR">'s Public Key that will be used by Medicity to authenticate the <"CLIENT\EHR VENDOR"> with the Medicity endpoint.

- Medicity will install the <"CLIENT\EHR VENDOR">'s public key into their certificate store.

- Medicity will supply the Medicity endpoint to the <"CLIENT\EHR VENDOR">. The <"CLIENT\EHR VENDOR"> will use the <"CLIENT\EHR VENDOR"> private key to authenticate to Medicity's endpoint.

Configuration

b. For <"CLIENT\EHR VENDOR"> to receive an XDR from Medicity:

- In exchange for the <"CLIENT\EHR VENDOR">'s endpoint, Medicity will send Medicity's Public Key that will\can be used by the <"CLIENT\EHR VENDOR"> to authenticate Medicity with the <"CLIENT\EHR VENDOR"> endpoint.

- The <"CLIENT\EHR VENDOR"> will supply the <"CLIENT\EHR VENDOR">'s endpoint to Medicity

Configuration

General Implementation Notes:

- ✓ A production domain is required. There are three options:
  a. The domain is a Medicity domain e.g. “CLIENTDOMAIN.medicity.net”
  b. The domain is a non-Medicity domain purchased and maintained by Medicity, e.g. “CLIENTDOMAIN.<com\org\net>”
  c. The domain is a non-Medicity domain purchased and maintained by the client. See section 4, “CLIENTDOMAIN to be purchased and maintained by the client” below.

- ✓ This will be the list of domain admins responsible for maintaining the provider directory under this requested domain.

- ✓ Medicity currently requires an attachment to be included CCD/CCDA document. *Secured Messages without an attachment may be available in a Future Medicity Release*

- ✓ XDR to Medicity WebDirect or iNexx message will appear in the inbox with subject name + “XDM/1.0/DDM” the CCDA will come over as an attachment in the form of an XDM zip file.

  XDM is a spec and the CCDA can be viewed by unzipping the file and opening the index.htm file and click on the CCDA link to view in human readable format.

Configuration

CLIENTDOMAIN to be purchased & maintained by the Client

Note: Only Applicable if domain is not @CLIENTDOMAIN.medicity.net

If the domain is purchased and maintained by the client, additional steps and information is required:

- Client must purchase the domain “CLIENTDOMAIN.<com\org\net>”
- Client must provide the following information for the CSR creation that will be done by Medicity
- Client must create corresponding MX record for “CLIENTDOMAIN.<com\org\net>” for smtp.medicity.net
- Client must create an SRV record for _ldap._tcp. “CLIENTDOMAIN.<com\org\net>” which points to medicity.net (204.246.142.220) on 10389

Configuration

Client\EHR vendor Next Steps:

After the CSR (usually a 24-hour turnaround) is created:

a. Medicity will email the Public IP and the CSR to the remote XDR client business and technical contacts.

b. Once the Public IP is received the domain must be mapped to this IP

c. The EHR vendor must set up Medicity as an endpoint and assign the EHR vendor's client certificate private key to the Medicity endpoint.

d. Once the CSR is received the client must purchase the SSL certificate for the domain name using the CSR provided.

Note: This is not the same Certificate as the endpoint certificate, it is required for the provider registry and domain

e. The SSL certificate must be emailed to HISPdeployment@medicity.com so Medicity can attach the SSL certificate to the Public IP for the domain name.

Configuration

Domain Admin Next Steps

XDR routing needs to be configured for the providers of the new domain. There are multiple configuration considerations:

a. All Sender addresses MUST be created in the “CLIENTDOMAIN” prior to sending a message. Medicity provides an upload capability. See section 9, “Upload provider directory process” for details.

b. All intended recipients must have a valid direct address found within the Medicity network or trusted HISP to HISP connections.

Configuration

c. Creating an Alias instead of provisioning a physical email addresses. – There are cases where physical addresses are not desired. Some EHRs, such as Epic, do not want to provision a physical mailbox for each provider within the “CLIENTDOMAIN”. Since there MUST be at least one physical direct email address setup on the domain to allow sending and receiving. An Alias can be setup to redirect email traffic for un-provisioned direct email addresses.

d. Assigning endpoints to physical direct email addresses. In the Medicity HISP provider Directory the remote XDR endpoints can be bound to an organizational address or individual provider address.

Note: by default iNexx is always bound to all addresses.

e. Organization level assignment - If the remote XDR endpoint is bound to the organization all the provider addresses in that organization will inherit the endpoint. If this is not desired, do not select XDR as an endpoint option for this organization

f. Provider level assignment – Providers can have a remote XDR endpoint bound to the physical address. This is additive to any other defined or inherited endpoints. A provider may have multiple endpoints if desired.

Confirmation

ATTACHMENT: Medicity Public Key

WHAT IS DUE: Confirmation that Settings are In Place

Note: While you are waiting on your endpoint to be built by Medicity, please apply the following configurations to your server/firewall to ensure that you are able to both send messages out to Medicity, as well as have the proper configurations applied to be able to receive messages from Medicity.

The attached Medicity Public key should be installed in all places where your security certificate (of which the public key was provided to Medicity) has been installed.

Below are the configuration requests:

- Medicity's Endpoint - https://xdr.medicity.net:20000/
- Open port 20000
- Medicity's "Public Key" certificate in a zip file used for authenticating Medicity to the client's XDR endpoint. (Meditech will need this for receiving XDR from Medicity.)

Confirmation

- ✓ Please change the extension zi_ to zip

- ✓ The following two IP needs to whitelist from Client:
  - 66.97.135.77 (this is the server IP where inbound XDR from client)
  - 206.71.83.107 (this is the server IP where outbound XDR to client)

There may be additional ports that need to be opened in addition to 20000 (that's 20,000) depending on your organization's setup. You will want to reach out to your vendor to confirm proper setup and answer EHR specific questions.

Testing

TASKS:

- ✓ Access the management console and webmail application, attend associated training, scheduled/provided by CliniSync
- ✓ CliniSync will provide an email containing details and links to support these activities
- ✓ Schedule testing session(s), coordinated by CliniSync
  - Recommend resources from networking and vendor attend at the beginning of the initial session with the hospital resource to ensure messages pass seamlessly
- ✓ Maintain issues/resolution log, CliniSync

DELIVERABLES:

- ✓ Provide testing call participant availability to CliniSync for scheduling

NEXT STEP:

- ✓ Selection of go-live date

Testing

Once your endpoint has been setup and the contact identified as the HISP Admin will receive a password reset to access your organization account through the management console and webmail application:

Management Console:	https://[client subdomain].medicity.net/?allowlogin=1
Webmail Application:	https://[client subdomain].medicity.net/webmail

To begin testing outbound from your EHR to Medicity, please use the following addresses:

Sending Address (from):	test.[client subdomain]@[client subdomain].medicity.net
Receiving Address (to):	karen.bishop@ohip.medicity.net

Testing

In order to address any issues or errors, please record the following information when testing so we are able to request a search of our error logs to assist with a remedy:

- Sending address
- Receiving address
- Date/time stamp
- Error received (or screen shot)

Please send an email outlining your issue, as a separate email, so I can forward to the proper resources.

If our resources are unable to remedy or identify that it may be an issue with your configuration, we can work to schedule a call with all necessary resources to attempt to complete the testing and finish the initial integration.

Please ensure that the following people are included on any possible call:

- Network resource
- Application (hospital) resource
- Vendor resource

Testing

Only if desired, a client can confirm that communications to Medicity are working from the EHR. Have the sending EHR system create an XDR and have the sending system configured to send using the following information:

Medicity XDR endpoint:	https://xdr.medicity.net:20000
Intended Recipient:	test.<CLIENTDOMAIN>@medicity.net
Set the Sender as:	test.sender@medicity.net

- Send a message as a *sender test.sender@medicity.net to test.<CLIENTDOMAIN>@medicity.net*.

- Also, send a follow-up email to *HISPdeployment@medicity.com* so that Medicity can confirm successful receipt of the test message.

Testing

Client Production testing steps:

- After Sections 1 through 6 have been completed, Production testing can begin.
- Medicity suggests that the remote XDR client send an XDR communication to an address specified by the XDR domain's admin.
- The XDR domain admin should verify that the XDR is received and confirm with the sender that the XDR was received.
- In the event that the XDR is not received, and all Domain and client EHR vendor setup has been confirmed to be setup correctly, submit a support request to HISPdeployment @medicity.com

Go-Live

TASKS:

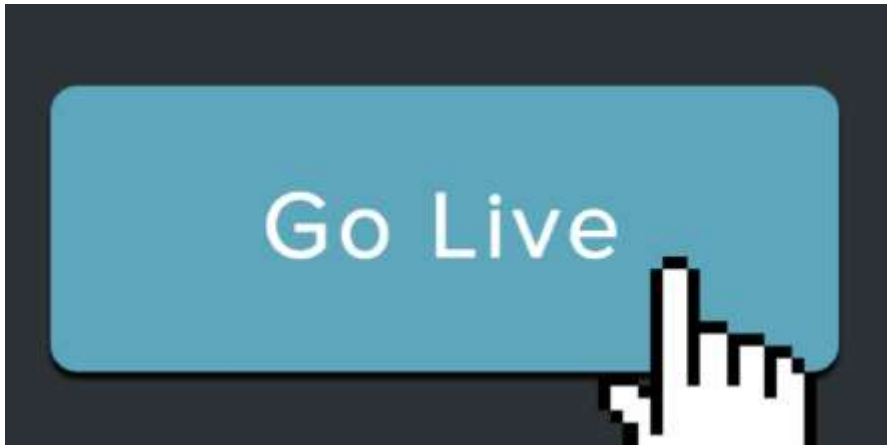
- ✓ Monitor outbound activity, reference materials provided by CliniSync
- ✓ CliniSync support portal access, initiated by CliniSync post go-live

DELIVERABLES:

- ✓ Provide a primary and secondary resource to CliniSync for communications moving forward

NEXT STEP:

- ✓ Alert CliniSync to any post go-live issues to include system updates or downtimes



Go-Live

Upload provider directory process:

- ✓ A batch upload spreadsheet will be provided, include direct addresses for sharing in the National Directory
- ✓ Provide the batch upload spreadsheet when you have new direct addresses to add to the National Directory
- ✓ Disable direct addresses as needed in your sub-domain