HISP Direct Integration

Contents

HISP OVERVIEW

A Health Information Service Provider (HISP) is an intermediary that routes Direct Secure Messages to and from your organization. When a HISP sends a Direct Secure Message, it will:

1. Use DNS (Domain Name System – A service that translates domain names into IP addresses) to look up the server that the HISP should send the message to and the certificate the HISP should use to encrypt the message.
2. Check whether the HISP trusts the recipient's digital certificate. If it doesn't, the HISP rejects the message.
3. Encrypt the message using the recipient's certificate.
4. Sign the message using the sender's certificate.
5. Send the message.

When a HISP receives a Direct Secure Message, it will:

1. Check that it trusts the certificate used to sign the message. If it doesn't, the HISP will reject the message.
2. Decrypt the message.
3. If it is a third party, use the domain part of the Direct address to determine which of its member organizations is the intended recipient and send the message to that organization.

CONNECTION SET-UP

This page contains information used in creating a new connection with a 3rd party. Netsmart uses MedAllies as a HISP for the CareConnect Inbox, more information can be found here: http://www.medallies.com/medallies-mail-tm-.html

CREATING A NEW HISP CONNECTION

For this connection, you will only need the Client's Direct Address. XDR endpoints and cert information are not needed for this setup. The Netsmart domain is 'netsmartdirect.net.' The following are the current test addresses:

- CareConnect Referrals: CareConnectTest@netsmartdirect.net
- CareConnect Inbox: CareConnectInboxTest@netsmartdirect.net

Direct Addresses are created based on the client being providing for:
[orgName]@netsmartdirect.net

Note: Some existing accounts may have old domains:
[orgName]@netsmart-direct.inpriva.net or [orgName]@uat.direct.ntst.com

Date	Modification	Modified By
1/9/2017	Initial Draft	Kayla Rowton

For questions, e-mail CConnect@ntst.com