§ 170.315(h)(1) Direct Project

Secure Direct Messaging with RFC-5751 Compliance

Overview

This documentation demonstrates compliance with **45 CFR § 170.315(h)(1) - Direct Project** . Our Health IT Module implements comprehensive Direct Project capabilities for secure transmission of encrypted and signed electronic health information to and from authorized Health Information Service Providers (HISPs).

The requirement ensures healthcare providers can securely exchange protected health information (PHI) using the Direct Protocol with cryptographic signing and encryption in accordance with federal security standards.

Woundtech

Requirement Details

Direct Protocol Implementation

Our Health IT Module implements Direct Project v1.2 for secure health information exchange with the following capabilities:

Required Enhanced Testing – Send

Requirement: The Health IT Module provides evidence and demonstration of successful send of encrypted and signed health information from the Health IT Module to three partners (e.g., other vendor Health IT Modules/HISPs that have implemented (h)(1) or (h)(2) capabilities).

Send Capability Documentation Includes:

- **RFC-5751 Wrapped Messages:** Documentation of Health IT Module sending "Wrapped" RFC-5751 encrypted and signed messages to three partner HISPs
- **Message Disposition Notifications (MDNs):** Documentation of Health IT Module receiving processed MDNs from each of the three partner HISPs, generated by partner HISPs upon receiving the Direct message
- Compliance with Direct Project: ONC Applicability Statement for Secure Health Transport, v1.2
- Cryptographic signatures and encryption per § 170.202(a)(2) standards

Required Enhanced Testing – Receive

Requirement: The Health IT Module provides evidence of successful receipt of encrypted and signed health information from three partners (e.g., other vendor Health IT Modules/HISPs that have implemented (h)(2) capabilities).

Receive Capability Documentation Includes:

- **RFC-5751 Wrapped Message Reception:** Documentation of Health IT Module receiving "Wrapped" RFC-5751 encrypted and signed messages from three partner HISPs
- **Message Processing:** Documentation that Health IT Module generates and sends processed MDNs that are transmitted to each of the three partner HISPs
- MDN generation upon successfully receiving Direct message from Health IT Module
- Compliance with Direct Project: ONC Applicability Statement for Secure Health Transport, v1.2

Standards & Regulations

Standard/Regulation	Description	Reference
Direct Protocol Version	Direct Project secure messaging specification for healthcare data exchange	Direct v1.2
RFC-5751 Specification	Secure/Multipurpose Internet Mail Extensions (S/MIME) version 3.2 for message wrapping	RFC 5751
Message Disposition Notification	Mechanism for reporting status of message delivery and processing	RFC 3798 (MDN specification)
Cryptographic Standards	Standards for encryption and digital signatures in Direct messaging	RFC 2630, RFC 3852 (CMS)
TLS Specification	Transport Layer Security for secure communication channels	RFC 2246, RFC 5246
Direct Applicability Statement	ONC guidance on Direct Project implementation for secure health transport	§ 170.202(a)(2), v1.2
HIPAA Security Rule	Federal requirements for protecting electronic protected health information	45 CFR § 164.312(a)(2)(i)

Implementation Details

RFC-5751 Message Wrapping

Our Health IT Module implements RFC-5751 S/MIME v3.2 message wrapping for secure Direct communication:

- ✓ **Message Encryption:** All health information messages are encrypted using AES-256 or equivalent encryption algorithms before transmission
- ✓ **Digital Signatures:** Messages are digitally signed using RSA-2048 or equivalent signatures to verify sender authenticity and message integrity
- ✓ **Wrapped Format:** Messages are wrapped in RFC-5751 S/MIME format for compatibility with Direct Protocol specifications
- ✓ **Certificate Validation:** HISP certificates are validated before encryption to ensure messages can be decrypted by intended recipients
- ✓ **Key Management:** Cryptographic keys are managed securely with appropriate key storage and rotation procedures

Message Disposition Notification (MDN) Processing

Our Health IT Module implements RFC 3798 MDN processing for message delivery confirmation:

- **MDN Generation:** Module generates MDNs upon successfully receiving Direct messages from partner HISPs
- **MDN Transmission:** MDNs are transmitted back to sending HISPs with appropriate delivery status indicators
- **MDN Parsing:** Module processes received MDNs from partner HISPs to confirm message delivery and processing status
- **Delivery Confirmation:** Delivery status is logged and made available to users for message tracking
- **Error Reporting:** MDNs include appropriate error indications if messages fail validation or processing

Cryptographic Standards

Our implementation utilizes industry-standard cryptographic algorithms:

- **Encryption:** AES-256 for message encryption
- **Digital Signatures:** RSA-2048 or RSA-4096 for message signing
- **Hash Algorithms:** SHA-256 or SHA-512 for integrity verification
- **Key Exchange:** Elliptic Curve Diffie-Hellman (ECDH) or RSA key exchange
- **Certificate Format:** X.509 v3 certificates for HISP identification

Direct Account Information

Direct Address

Healthcare providers and other entities can send encrypted Direct messages to our Health IT Module using Direct addresses. Direct addresses follow standard format: **username@directaddress.com**

Certificate Management

Our Health IT Module maintains X.509 certificates for Direct messaging:

- Certificates are obtained from approved Direct Certificate authorities
- Certificates contain organization information and Direct address binding
- Certificate revocation status is checked before sending messages
- Certificate renewal is performed before expiration
- Old certificates are securely archived per compliance requirements