§ 170.315(b)(1) Transitions of Care

Direct Edge Protocol Documentation

Overview

This documentation demonstrates compliance with **45 CFR § 170.315(b)(1) - Transitions of Care**. Our Health IT Module supports secure transmission of electronic health information using Direct Project protocols and Edge Protocol implementation for SMTP connections.

The requirement ensures healthcare providers can securely send and receive protected health information (PHI) using encrypted, authenticated connections that meet federal security standards.

Woundtech

Requirement Details

Send Using Edge Protocol for SMTP

Our Health IT Module sends health information using the SMTP (Simple Mail Transfer Protocol) with Edge Protocol implementation for secure, encrypted transmission of electronic health information.

Our Health IT Module provides documentation of the ability to:

- **Connect using valid cipher suites** in accordance with RFC 5321 and subsequently updated standards (RFC 2246, RFC 7465, NIST SP 800-52 Revision 1)
- **Establish STARTTLS connections** and reject connections upon sending to HISP (Health Information Service Provider) with invalid certificates
- Validate server certificates during STARTTLS handshake to ensure secure, authenticated communication
- Comply with § 170.202(d) ONC Implementation Guide for Direct Edge Protocols, v1.1
- Comply with § 170.202(a)(2) Direct Project: ONC Applicability Statement for Secure Health Transport, v1.2
- Support SMTP Test requirements for certificate validation and rejection procedures

Standards & Regulations

Standard/Regulation	Description	Reference
SMTP Protocol	Simple Mail Transfer Protocol specification for email sending	RFC 5321
TLS Specification	Transport Layer Security protocol for encrypted connections	RFC 2246
Cipher Suite Restrictions	Prohibits NULL encryption cipher suites for enhanced security	RFC 7465
NIST TLS Guidelines	NIST recommendations for TLS implementation and cipher suites	NIST SP 800-52 Revision 1
Direct Edge Protocols	ONC implementation guide for Direct Edge Protocols (SMTP protocol specified)	§ 170.202(d)
Direct Applicability	Direct Project ONC Applicability Statement for Secure Health Transport	§ 170.202(a)(2), v1.2
SMTP Test Method	ONC test requirement for SMTP Edge Protocol implementation validation	SMTP Test

Regulatory Authority: 45 CFR § 170.315(b)(1) requires Health IT Module to support receiving electronic health information securely using Direct Protocol and Edge Protocol implementations with proper certificate validation and encryption standards.

Implementation Details

STARTTLS Connection Security

- ✓ **SMTP STARTTLS Support:** Module supports STARTTLS command to upgrade plain SMTP connections (port 587) to encrypted TLS sessions
- ✓ **Certificate Validation:** Module validates server certificates presented by HISP during STARTTLS handshake for authenticity and validity before sending
- ✓ **Invalid Certificate Rejection:** Module immediately rejects connections when certificates are invalid, expired, self-signed, or untrusted from an untrusted certificate authority
- ✓ **Secure Data Transmission:** Module terminates SMTP connections on certificate validation failure, preventing any unencrypted or insecure transmission of protected health information
- ✓ **Connection Timeout:** Failed authentication and certificate validation attempts result in connection termination with appropriate timeout periods to prevent brute force attacks

SMTP Protocol Support

Our Health IT Module implements comprehensive SMTP protocol support including:

- **STARTTLS Command:** Initiates TLS encryption upgrade on standard SMTP submission port 587
- **AUTH Command:** Authenticates user after successful STARTTLS connection establishment
- **EHLO Command:** Advertises server capabilities including STARTTLS and authentication support
- **MAIL Command:** Specifies sender of health information message
- **RCPT Command:** Specifies recipients for health information transmission
- **DATA Command:** Transmits health information messages to HISP
- **QUIT Command:** Gracefully closes SMTP connection

TLS Version Support

In accordance with NIST SP 800-52 Revision 1 recommendations, our implementation supports:

- **TLS 1.2** (minimum recommended version)
- **TLS 1.3** (where applicable)

Note: TLS 1.0 and 1.1 are deprecated per NIST guidelines.

Cipher Suite Compliance

Cipher suites are carefully selected per RFC 7465 and NIST SP 800-52 Revision 1. All NULL encryption cipher suites are strictly prohibited. Only high-security, industry-standard cipher suites suitable for healthcare data transmission are supported, including:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256