Cisco Voice over IP (VoIP) Compliance for the Health Insurance Portability and Accountability Act (HIPAA)

What information is protected

The Privacy Rule protects all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "Protected Health Information (PHI)."[3] It includes:

- The individual's past, present, or future physical or mental health or condition
- The provision of health care to the individual, or
- The past, present, or future payment for the provision of health care to the individual

Benefits

How HIPAA affects VoIP:

- **Stored data,** such as voicemails and call recordings, are not excluded by section 160.103 of the Security Rule,[8] as they must be protected against unlawful disclosure
- **Transmitted call meta data** can include information which may lead to re-identification of an individual, in direct contravention of section 164.514 of the HIPAA Privacy Rule[4]
- **Transmitted voice data** is not covered by HIPAA[11]

© 2019 Cisco and/or its affiliates. All rights reserved.

How does HIPAA apply to VoIP?

As part of the Health Insurance Portability and Accountability Act (HIPAA), the **Privacy Rule** exists to ensure that individuals' health information is properly protected, while allowing the flow of health information needed to provide and promote high-quality healthcare and to protect the public's health and well-being. The Privacy Rule applies to any healthcare provider (the covered entity) or business associate who **transmits health information in electronic form** in connection with transactions for which the Secretary of Health and Human Services (HHS) has adopted standards under HIPAA[1].

Encryption and IP telephony

To protect unlawful disclosure of e-PHI, the HIPAA Security Rule requires adequate transmission security by encryption. It states:

"Transmission Security. A covered entity must implement technical security measures that guard against unauthorized access to e-PHI that is being transmitted over an electronic network."[7]

"Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate."[7]

IP telephony utilizes industry-standard encryption mechanisms such as TLS 1.2 to encrypt SIP traffic to and from VoIP handsets. TLS 1.2 is recognized as a secure, reasonable, cost-effective, and efficient method for the protection of VoIP traffic.

Concerning TLS version support, the National Institute of Standards and Technology states in its Special Publication, "800-52 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations"[9]:

"This Special Publication provides guidance to the selection and configuration of TLS protocol implementations while making effective use of approved cryptographic schemes and algorithms. In particular, it requires that TLS 1.1 be configured with cipher suites using approved schemes and algorithms as the minimum appropriate secure transport protocol. It also recommends that agencies develop migration plans to TLS 1.2, configured using approved schemes and algorithms, by January 1, 2015.

TLS 1.1 was developed to address discovered weaknesses in TLS 1.0, primarily in the areas of initialization vector selection and padding error processing."

Further to this, the Internet Engineering Task Force (IETF) clearly states in section 4 of its draft memo,[10] "Deprecating TLSv1.0 and TLSv1.1":

"TLSv1.0 MUST NOT be used. Negotiation of TLSv1.0 from any subsequent [sic] version of TLS MUST NOT be permitted. Any version of TLS is more secure than TLSv1.0 and can be configured to prevent interception..."

References

1. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf
2. https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html
3. https://www.govinfo.gov/content/pkg/CFR-2010-title45-vol1/pdf/CFR-2010-title45-vol1-sec160-103.pdf
4. https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#protected
5. https://www.hhs.gov/hipaa/for-professionals/security/index.html
6. https://www.govinfo.gov/content/pkg/CFR-2010-title45-vol1/pdf/CFR-2010-title45-vol1-sec164-306.pdf
7. https://www.govinfo.gov/content/pkg/CFR-2010-title45-vol1/pdf/CFR-2010-title45-vol1-sec164-312.pdf
8. https://www.govinfo.gov/content/pkg/CFR-2010-title45-vol1/pdf/CFR-2010-title45-vol1-sec160-103.pdf
9. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf
10. https://tools.ietf.org/id/draft-moriarty-tls-oldversions-diediedie-00.html
11. Under 106.103 voice via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission

© 2019 Cisco and/or its affiliates. All rights reserved.

Learn more

About upgrading your phone security to TLS 1.2 to be compliant with HIPAA today.

Organizations that fail to comply with these regulations run the risk of fines or criminal charges. For more details on security and compliance, visit Cisco.com/go/voipcompliance.

Recommendations

The collaboration environment, including software, voice endpoints, and video endpoints, should be updated to support TLS 1.2.

Cisco collaboration software

To support TLS 1.2, administrators should update the collaboration environment to software release 11.5.1 (SU3), and contact center software to release 11.6(1).

A software upgrade is required for the following applications:

- Cisco® Unified Communications Manager
- Cisco Unified Contact Center Enterprise solutions
- Cisco Unified Contact Center Express solutions
- Cisco Customer Journey Platform
- IM and Presence
- Cisco Unity® Connection
- Cisco Prime® Collaboration Deployment for releases earlier than 11.5.1 (SU3)

Cisco voice endpoints

Legacy Cisco IP phones

Replace any legacy Cisco IP phones (6900, 7900, 8900, and 9900 Series) with newer models, such as the 7800 or 8800 Series. The 7800 and 8800 Series phones support TLS 1.2. For more information, see the Cisco Endpoints portfolio page.

Cisco IP Phone 7800 Series and 8800 Series

Cisco IP Phone 7800 Series and 8800 Series should be upgraded with firmware release 12.1 in order to support TLS 1.2.

For more details on security improvements in the latest Cisco IP phones, refer to the Cisco IP Phone 7800 and 8800 Series Security Overview.

Cisco video endpoints

Legacy Cisco TelePresence

Newer TANDBERG™ Codec (TC) endpoints support collaboration endpoint software (CE) release 9.1(3).

For legacy TC endpoints such as the C-Series, EX, MX200 or MX300 G1, or Profile, consider upgrading to Cisco TelePresence® TC software release 7.3(11).

Legacy immersive systems such as the TX9000 Series and Cisco TelePresence System will not support TLS 1.2.

Cisco collaboration endpoint software

Consider upgrading any CE endpoints (Cisco DX70 or DX80 or Cisco TelePresence MX200 or MX300 G2, MX700 or MX800, or SX Series) to Cisco CE software release 9.1(3).

*Note: Cisco DX650 endpoints on Android should be replaced with newer hardware.

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

C45-742608-00 07/19