Achieve Email Compliance with the HIPAA & HITECH Acts

A white paper by:
West Wind Technology Solutions

Health-related organizations and even their business associates need to pay more attention now to email compliance. Penalties can reach up to $250,000 per violation plus 10 years of imprisonment, so it would be foolish not to.

HIPAA requirements that affect email

Before you can start working on achieving email compliance, you have to identify first the specific HIPAA standards you need to comply with. The specific standards affecting email systems can be found in the **Technical Safeguards** section of the **HIPAA Security Rule**. These standards are namely:

1. **Access Controls**. A covered entity must implement technical policies and procedures limiting access to systems containing electronic protected health information (ePHI) only to personnel with sufficient access rights (§ 164.312 (a))
2. **Audit Controls**. A covered entity must implement software that record and examine activity in information systems that contain or use ePHI. (§ 164.312 (b))
3. **Integrity**. A covered entity must implement policies and procedures to protect ePHI from improper alteration or destruction. (§ 164.312 (c))
4. **Person or entity authentication**. A covered entity must implement procedures to verify that a person or entity seeking access to ePHI is the one claimed. (§ 164.312 (d))
5. **Transmission security**. A covered entity must implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.

Some of the implementation specifications laid down to address those standards involve:

- unique user identification
- a mechanism to authenticate ePHI and to corroborate that ePHI has not been altered or destroyed in an unauthorized manner
- security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of
- encryption of ePHI

How important is email encryption?

At this point, we’d like to divert our attention a little and focus on encryption of ePHI. In the complete HIPAA documentation, it appears in the implementation specifications of two standards: Access Controls and Transmission Security. But in both cases, it is only classified as an “addressable” implementation specification.

… addressable?

You see, HIPAA classifies each implementation specification as either “required” or “addressable”. Implementation of a specification labeled as “required” is, as the term suggests, mandatory. This might mislead you to think that, being an “addressable” specification; it might only be optional and hence shouldn’t be given too much importance.

However, we should be careful in interpreting the word “addressable”, for it does not mean “optional”. According to HIPAA: If an implementation specification is labeled “addressable”, then you must assess whether the specification is a reasonable and appropriate safeguard for protecting ePHI.

If you find the implementation specification reasonable and appropriate, then you should implement it. Otherwise, you will have to document why it wouldn’t be reasonable and appropriate to implement and then find an alternative that is.

Because the contents of a regular email are stored and transmitted as plain text and because copies of those contents are normally stored in multiple places (your computer, your mail server, each recipients’ computers and mail servers), they can be very vulnerable to unauthorized access. Encryption prevents that. It should therefore be reasonable and appropriate to implement email encryption to guard against unauthorized access to ePHI.

Email encryption helps in attaining HIPAA and HITECH compliance

When your email message is encrypted, it won’t matter if it gets intercepted by malicious individuals. They won’t be able to modify it or disclose the information stored inside. Highly confidential information like ePHI can only be accessed by the intended recipient. Thus, individually identifiable health information will be kept confidential.

Remember that one of the main objectives of HIPAA is to prevent unauthorized disclosure of individually identifiable health information. Encryption easily achieves this. Simple and powerful email encryption is a key ingredient in helping you achieve HIPAA and HITECH compliance.

Contact Matthew Sisson with West Wind Technology Solutions at (269) 217-0831 or msisson@westwindts.com for a consultation today!

WEST WIND
Technology Solutions
www.westwindts.com

References:

INFO - http://www.sendinc.com/blog/2011/06/how-to-achieve-email-compliance-with-the-hipaa-hitech-acts/