# Regulatory Compliance with HIPAA

May 2013

## HIPAA AND TECHNOLOGY

HIPAA is a federal law that protects personal health information while giving health care providers and related operations access to necessary information. HIPAA has several provisions that guide its administration and enforcement, including some relevant to health information technology and the electronic exchange of health information: the Privacy Rule, the Security Rule, and the HITECH Act.

## HIPAA'S PRIVACY RULE, SECURITY RULE, AND HITECH ACT

**Privacy Rule**: applies to protected health information (PHI) in all forms (paper, oral, electronic, etc.). It requires covered entities to institute safeguards for protecting PHI, but it does not discuss the cases in which PHI can be used, when authorization is required and patients' rights.

*More information: Summary of Privacy Rule.*

**Security Rule**: applies **only** to PHI in electronic form (E-PHI).The Security Rule sets standards on the processes and security measures that should be taken to keep PHI private. It discusses safeguards that protect E-PHI from unauthorized access, alteration, deletion and transmission (page 8335). Under the Security Rule, faxes, telephone calls, video teleconferencing, and voicemail are not E-PHI because they do not exist in electronic form before the transmission. Thus, those activities are not covered by the Security Rule (page 8342), but they are covered by the Privacy Rule.
*More information: The Security Rule 101 Overview, Security Rule Guidance Material*

The **HITECH Act** specifies levels of violations and penalties for violations of the HIPAA rules. It also requires periodic audits to ensure that covered entities and business associates are complying with the Privacy and Security Rules and Breach Notification.
*More information: HITECH modifications to privacy and security*

## WHAT DOES HIPAA MEAN FOR VIDEOCONFERENCING?

Videoconferencing may involve the electronic exchange of PHI, which is protected under HIPAA law. Security considerations with videoconferencing may include ensuring that unauthorized third parties cannot record or listen to a videoconference, making sure recorded videoconferences are securely stored and properly identified, having a procedure for initiating and receiving video calls, and setting up protocols for text chat, screen-sharing, and file-transfer. Videoconferencing is just one aspect of many to consider when establishing and maintaining HIPAA-compliant IT security standards.

## HOW DOES ZOOM HELP YOU TO COMPLY WITH THE HIPAA?

Zoom has several characteristics that make it easier to protect health information:

**1. Infrastructure:**
Zoom's communications infrastructure for real-time video, audio and data communications leverages Amazon Web Services. Amazon Web Services provides a highly reliable, scalable, secure infrastructure platform in the cloud that powers hundreds of thousands of businesses in 190 countries around the world.For information on Amazon EC2,please see http://aws.amazon.com/what-is-aws/; for information on AWS Security, see http://aws.amazon.com/security/.

**2. Communications:**
A distributed network of low-latency multimedia routers (software) resides on Zoom's communications infrastructure. With these low-latency multimedia routers, all session data originating from the host's device and arriving at the participants' devices is dynamically switched — never stored persistently through the Zoom communications infrastructure. Zoom sessions are completely temporary and operate analogously to the popular mobile conversation over the public mobile network.

**3. Encryption:**
Zoom can secure all session content by encrypting the communications channel between the Zoom client and the multimedia router using a 128-bit Transport Layer Security (TLS) encryption tunnel. Zoom meeting participants connect to the Zoom communications network via a dedicated logical connection. This connection is strictly controlled by the Zoom client and is dedicated exclusively to session communications – no other tasks outside of what the meeting client allows.

**4. Local Recorded Media Storage:**
Zoom allows users to record e-PHI videoconferences. These files are always stored on a user's computer or HIPAA-compliant EHR system, and are never stored on Zoom servers or accessible to Zoom.

## DOES DATA HAVE TO BE ENCRYPTED TO BE HIPAA COMPLIANT?

The Security Rule does not require encryption if an entity can prove it is not reasonable or appropriate to do so. However, it is a good idea to encrypt data whenever possible because, in the event of a breach, proper encryption exempts HIPAA-covered entities from the Breach Rule (HITECH Act section 13402), which requires notification of PHI that has not been secured (i.e. encrypted) according to the security guidance publication (74 FR 19006).

Encryption processes that have been tested and meet the guidance standard:

(i) "Valid encryption processes for data at rest are consistent with NIST Special Publication 800–111, Guide to Storage Encryption Technologies for End User Devices." (p. 19009-10)

(ii) "Valid encryption processes for data in motion are those that comply with the requirements of Federal Information Processing Standards (FIPS) 140–2. These include, as applicable, standards described in NIST Special Publications 800–52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800–77, Guide to IPsec VPNs; or 800–113, Guide to SSL VPNs, and may include others which are FIPS 140–2 validated." (p. 19009-10)

**Zoom's communications layer can be encrypted with 128-bit Transport Layer Security (TLS) and application layer with AES 128 bits encryption. Zoom does not store any of your data.**

## WHO MUST COMPLY WITH HIPAA?

Not all operations that handle health-related information must follow HIPAA law (including many schools, state agencies, law enforcement agencies, and municipal offices). Under HIPAA the groups that must follow HIPAA rules are:

1. Covered entities: health care providers, health plans, and health clearinghouses.
2. Business associates: a person or group providing functions or services for a covered entity and require access to identifiable health information. For example, a CPA firm, an attorney, or an independent medical transcriptionist. Business associate FAQs

**Zoom Video Communications does not fall under either group that must comply with HIPAA.**

## IS A SOFTWARE VENDOR A BUSINESS ASSOCIATE UNDER HIPAA?

It depends. If a vendor or subcontractor has routine access to PHI, it is considered a business associate. For example, a vendor that hosts software containing patient information on its own server or accesses patient information when troubleshooting the software is considered a business associate and must have a business associate agreement with the covered entity (HIPAA Privacy Rule 45 C.F.R. § 164.504(e)).

The only exception under HITECH section 13408 is in the case of data transmission organizations that only transport information but do not access it, such as the US Postal Service, Internet service providers, and telecommunications companies. While these entities may have access to PHI, they only access it randomly or infrequently as necessary or as required by law (page 22).

**Zoom never has access to any information, health or otherwise, that you may observe, transmit, or receive by using Zoom, and therefore is not a business associate under HIPAA rules.**

*More information: U.S. Department of Health on Software Vendors, U.S. Department of Health on Conduits*

## IS ZOOM HIPAA COMPLIANT?

Zoom is neither a covered entity nor a business associate. We do not have access to any identifiable PHI of a covered entity that may use our services. Therefore, we do not fall under HIPAA compliance rules. Zoom helps your program or organization be HIPAA compliant. (Please see section “How does Zoom help you to comply with HIPAA?”)

## IS ZOOM HIPAA CERTIFIED?

Certification of health technology is regulated under the HITECH Act, which does not certify software and off-the-shelf products(page 8352 of the Final Security Rule), set criteria for certification, or accredit independent agencies that do HIPAA certifications. In short, third-party HIPAA certification groups you may use are not regulated by any federal accreditation agency.

Currently HITECH only provides for the testing and certification of Electronic Health Records (EHR) programs and modules. The certification is generally used to qualify health operations for Medicare and Medicaid EHR Incentive Programs. Zoom is not an EHR software or module, and therefore is not certified.

*More information: The permanent certification program fact sheet, Authorized EHR testing and certification bodies.*

## DOES ZOOM OFFER A HIPAA BUSINESS ASSOCIATE CONTRACT?

No. Zoom does not have any access to the identifiable health information of a covered entity that may use its services. Therefore, Zoom is not a business associate under HIPAA rules and does not need to enter into a business associate agreement with a covered entity to be used. (See “Is a software vendor considered a business associate under HIPAA?”)

*More information: U.S. Department of Health on Business Associate Agreements*

**Zoom never has access to any information, health or otherwise, that you may observe, transmit, or receive by using Zoom, and therefore is not a business associate under HIPAA rules.**

*More information: U.S. Department of Health on Software Vendors, U.S. Department of Health on Conduits*

## MORE INFORMATION:

HIPAA (Health Insurance Portability and Accountability Act of 1996), Public Law 104-191, the complete suite of HIPAA Administrative Simplification Regulations are found at 45 C.F.R. Part 160, Part 162, and Part 164.

Privacy Rule “Standards for Privacy of Individually Identifiable Health Information” and is found at 45 CFR Part 160 and Subparts A and E of Part 164.

Security Rule “Security Standards for the Protection of Electronic Protected Health Information” is found at 45 CFR Part 160 and Subparts A and C of Part 164.

HITECH - Health Information Technology for Economic and Clinical Health Act.

Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules are found at 45 C.F.R. Parts 160 and 164.