HIPAA and Privacy

What to consider when building real-time cloud-based voice and messaging applications

Introduction

The billion-dollar healthcare industry, allied to the growth of cloud platforms, gives providers a huge opportunity to boost revenue by offering enhanced applications with real-time voice and messaging capabilities. But to take advantage of this opportunity, it's essential that healthcare providers fully understand, and comply with, the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act.

That's why Aculab recently announced conformance to HIPAA and HITECH regulations, which allows us to enter into HIPAA Business Associate Agreements (BAA) with our Covered Entity customers who provide healthcare platforms. The purpose of this mini-paper is to highlight what it means to you and why it's so important.

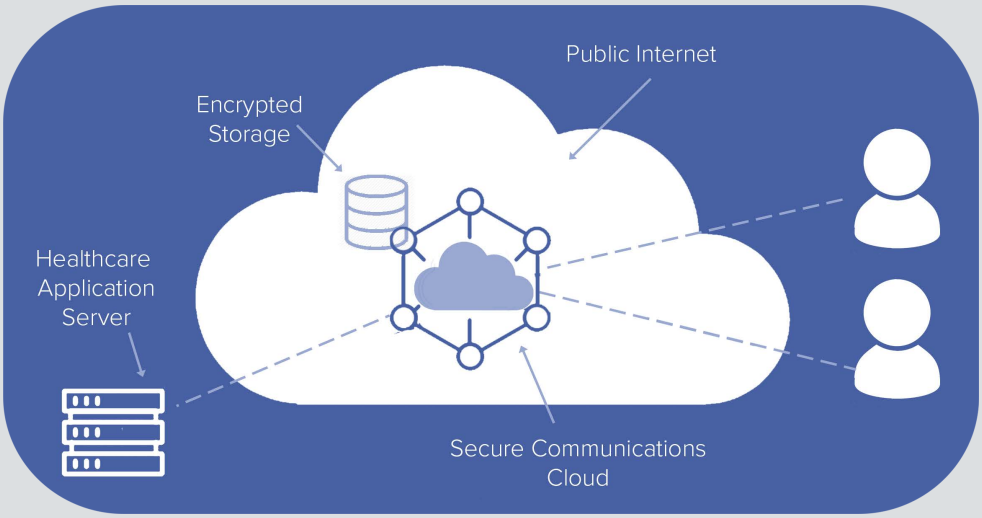
HIPAA and Privacy

What to consider when building real-time cloud-based voice and messaging applications

What are HIPAA and HITECH regulations?

The HIPAA of 1996 was introduced to improve the efficiency and effectiveness of the healthcare system in the US, including national standards for electronic healthcare transactions and code sets, unique health identifiers, and security. At the same time, it mandates privacy protections for individually identifiable health information. The HIPAA Rules apply to Covered Entities and Business Associates (see below).

HITECH came into effect in February 2009 and promotes the adoption and meaningful use of health information technology. It also addresses the privacy and security concerns associated with the electronic transmission of health information.



Why is it so important?

A HIPAA BAA is essential for anyone considering using a cloud-based Communications Platform-as-a-Service (PaaS), such as Aculab Cloud, as part of the solutions it offers to healthcare service providers in the United States. Any business offering patient management and advisory (PMA) or electronic healthcare records (EHR) solutions is obliged to ensure compliance with the HIPAA Privacy and Security Rules.

Quite simply, if you want to use a cloud communications API platform to add real-time voice and messaging to your applications, then you need to ensure its use complies with HIPAA and HITECH rules. Only Aculab Cloud makes this possible.

What is a Covered Entity/Business Associate?

Covered Entities encompass health plans, healthcare clearing houses, and healthcare providers that electronically transmit any form of health information included under US Department of Health & Human Services standards. A Business Associate is any organisation or person working with, or providing services to, a Covered Entity that handles or discloses Personal Health Information (PHI) or Personal Health Records (PHR).

Individuals, organisations, and agencies meeting the definition of a Covered Entity under HIPAA must protect the privacy and security of health information and provide individuals with certain rights with respect to their health information. If a Covered Entity engages a Business Associate to help it carry out its healthcare activities and functions, it must have a written Business Associate contract to ensure the Business Associate also complies with the Rules' requirements.

"Quite simply, if you want to use a cloud communications API platform to add real-time voice and messaging to your applications, then you need to ensure its use complies with HIPAA and HITECH rules. Aculab Cloud makes this possible."

HIPAA and Privacy

What to consider when building real-time cloud-based voice and messaging applications

The HIPAA and Security Rules - Privacy rules

The Privacy Rule addresses the use and disclosure of individuals' PHI by Covered Entities or Business Associates. It ensures that individuals' health information is properly protected, while permitting the disclosure of health information needed for high quality healthcare and to protect the public's well-being. Further standards within the Rule provide for individuals' rights to understand and control how their health information is used.

Security Rule

The Security Rule encompasses federal safeguards for protecting PHI in electronic form (e-PHI), and must be applied by Covered Entities and their Business Associates to ensure the confidentiality and integrity of e-PHI. The Rule allows the adoption of technologies to improve the quality and efficiency of patient care, such as those used in PMA, EHR, pharmacy and laboratory systems.

What is considered PHI?

In essence, PHI is information that relates to the individual's health condition, or the provision of healthcare to the individual, that identifies, or can be used to identify, the individual.

How do the rules apply to Aculab?

The PMA and EHR services provided by Aculab's customers clearly include management and administration services, both of which are included in the list of services identified in the Privacy Rule, and the transmission of e-PHI. Customers use Aculab Cloud for a variety of solutions, including those involving patient management, advisory, care, diagnosis, results, rehabilitation, messenger, and information systems.

Aculab, as the operator of Aculab Cloud is not a Covered Entity and Aculab's healthcare customers may not be Covered Entities. However, an Aculab customer performing functions or activities that involve the use or disclosure of e-PHI, by providing services to a Covered Entity is, by definition, a Business Associate.

The relationship between a Covered Entity and a Business Associate is through a BAA. In the case of a service provider to a Business Associate, the service provider becomes a Business Associate and, for the purpose of the BAA, the other party becomes a Covered Entity. That means Aculab is the Business Associate and its customer is the Covered Entity.

HIPAA and Privacy

What to consider when building real-time cloud-based voice and messaging applications

Suggestions for Ensuring Compliance

The following list provides some high-level suggestions for achieving compliance with the HIPAA Privacy and Security Rules when using a platform, such as Aculab Cloud, to process and transmit e-PHI involved in a PMA or EHR solution.

Authentication

Password authentication to access data such as recordings, voicemail messages or voice response systems doesn't alter the fact that such data is e-PHI and, if it is created, received, processed, stored or transmitted via Aculab Cloud, it is subject to the Privacy and Security Rules. However, that is a good method of ensuring compliance, as applying protective measures is the essence of the Rules' requirements.

Encryption

Whether or not the data is voice or speech and broadcast or transmitted over encrypted channels, it remains e-PHI and is subject to the Rules. Encrypting the data is not a means of avoiding your obligation; it is merely an effective means of complying with the Rules and meeting your obligation.

SMS

You can't send a short message over an encrypted channel; it remains plain text on transmission. Furthermore, an SMS sent to the patient includes the destination number, which could be used to identify the individual, thus qualifying the text as e-PHI. So, you need to ensure that the content of text messages contains no sensitive patient data. A message stating "Your appointment for tomorrow at 10:15 is confirmed" is compliant, whereas a message stating "Your appointment at the <insert too much information> clinic..." would not be.

Recordings

Voice recordings can be made by healthcare professionals and patients alike, and are subject to compliance. An effective method of protecting and securing recordings is to encrypt the file. However, there are further considerations around how you handle the encryption. For example, the encrypted file and the encryption key should never be sent via the same route, nor retained by the platform after use. The key should be received by the platform only when needed at the time of use, never stored on the platform, and destroyed after use, simultaneously with transmission of the encrypted file. The source recording should also be deleted.

Message Playback

The process is similar, albeit in reverse, for playback of a .wav file, for example, to relay information in the form of a message to a patient. On receipt of the encrypted file for transmission, you should ensure the applicable key is available only at the time of decryption in order to play the message back. As above, the key should be received via a different route from the message and destroyed after use, along with the original encrypted message.

Fax Handling

The process is similar when sending fax messages, the use of which technology is still widespread in healthcare for the transfer of health records. On receipt of the encrypted fax for transmission, you should ensure the applicable key is available only at the time of decryption in order to transmit the fax. Again, the key should be received via a different route and destroyed after use, as with the original encrypted message. It's the reverse for receiving a fax and forwarding the corresponding encrypted message to the intended receiver.

About Aculab

Aculab provides deployment proven telephony products to the global communications market

Whether you need telephony resources on a board, on a host server processor or from a cloud-based platform, Aculab ensures that you have the choice. We are an innovative, market leading company that places product quality and support right at the top of our agenda. With over 35 years of experience in helping to drive our customers' success, our technology is used to deliver multimodal voice, data and fax solutions for use within IP, PSTN and mobile networks – with performance levels that are second to none.

For more information

To learn more about Aculab Cloud and Aculab's extensive telephony solutions visit:

www.aculab.com

Contact us

Phone
+44 (0) 1908 273800 (UK)
+1 (781) 352 3550 (USA)

Email
info@aculab.com
sales@aculab.com
support@aculab.com

Social
@aculab
aculab