HIPAA-Compliance for Dental Care Voice Applications

Dental practice and industry partners often demand quick and easy communication between providers, care team, patients, and others. This communication is usually messages that go through traditional texting or email applications. Convenient worry-free communication and optimized workflow are essential.

But this communication is vulnerable to interception and should be within a protected environment, one that preferably caters to the fast-paced world of dental practice.

There are already applications that allow dental providers, colleagues, and patients to communicate within a secure environment. Still, they lack texting efficiency, are tedious, and often do not support continued conversation and collaboration.

More importantly, they do not support or integrate with conversational AI platforms and virtual assistants that answer dental care questions, deliver care reminders, send messages, capture and retrieve patient data, schedule appointments, order automatically from suppliers, and perform many other tasks through the power of voice and conversational interfaces.

The use cases for the integration of secure texting and virtual assistants on AI platforms are many in dental care. This machine learning translates to an improved workflow, improved outcomes, and automatic documentation.

The idea of a smart, always-available, hands-free, secure text and voice-powered virtual assistant in healthcare is hardly new, but as interest in virtual assistants gains steam in the dental industry, so has a concern about data privacy and security. In a survey published by Microsoft in April 2019, 41 percent of voice assistant users said they were concerned about privacy and security.

In this white paper, we will explain why HIPAA compliance matters. Then we will summarize the key components of HIPAA privacy protection and reference supporting systems,

agreements, policies, frameworks, and methods that a secure texting and conversational AI platform uses.

We will then describe best practices for creating secure text and voice applications with a conversational AI platform that goes beyond HIPAA requirements and concludes with general implementation steps for creating secure texting and voice using a conversational AI platform.

Why HIPAA Matters

HIPAA applies to the storage, use, and disclosure of a patient's individually identifiable health information. Failure to comply with HIPAA can have severe consequences. Suppose protected health information is used or disclosed in a way that does not comply with HIPAA. In that case, a dentist may need to notice the impermissible use to the affected individuals, the federal government, and, if more than 500 individuals are affected, the media. The federal government has stepped up HIPAA enforcement, conducting more audits and seeking more financial penalties from violators.

HIPAA

Unfortunately, data breaches are all too common, and their repercussions are very serious for the patients and the responsible provider or organization. They must answer to the agencies that enforce the laws for data privacy and security.

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and its subsequent extensions and modifications, are the set of U.S. laws that are designed to prevent breaches of Protected Health Information ("PHI") handled by health insurance providers, healthcare providers, doctors, and hospitals ("Covered Entities") or their third-party service providers ("Business Associates"). HIPAA is administered and regulated by the U.S. Department of Health and Human Services (HHS) Office for Civil Rights ("OCR").

PHI is any healthcare information, including medical and dental diagnoses, lab reports, vital data measurements, drug prescriptions, and more, that can be identified to an individual by what HIPAA refers to as "Identifiers."

Identifiers include:

- Names
- Dates, except the year
- Telephone numbers
- Geographic data
- FAX numbers
- Social Security numbers

- Email addresses
- Medical record numbers
- Account numbers
- Health plan beneficiary numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plates
- Web URLs
- Device identifiers and serial numbers
- Internet protocol addresses
- Full face photos and comparable images
- Patient partial images with unique identifiable marks or characteristics
- Biometric identifiers (i.e., retinal scan, fingerprints, voiceprints)
- Any unique identifying number or code

HIPAA law includes the Privacy Rule and Security Rule.

Privacy Rule

The HIPAA Privacy Rule ("Privacy Rule") includes regulations to limit PHI's use and disclosure. The Privacy Rule requires doctors to provide patients with an account of each entity to which healthcare providers disclose PHI for administrative purposes while still allowing relevant health information to be used within the proper context and authorized channels.

Specific safeguards are required to be in place to protect PHI, and there are set limits and conditions regarding the use and disclosure of data without patient authorization. The Privacy Rule also gives patients the right to access their health information. The Privacy Rule applies to all PHI, including physical media and records, as well as electronic PHI ("ePHI").

The Security Rule

The HIPAA Security Rule establishes national standards to protect PHI created, received, processed, or maintained by, or on behalf of, a covered entity. The Security Rule requires appropriate administrative, physical, and technical safeguards. These safeguards are based on the Security Rule requirements, risk assessments, and application of industry-standard security controls.

The Security Rule applies to health plans, healthcare clearinghouses, and any healthcare provider who transmits health information in electronic form. Below are the various safeguards.

Administrative Safeguards
The Administrative Safeguards establish the administrative processes and procedures for an organization's HIPAA-compliance. They are broken down into standards:

- Security management process

- Assigned security responsibility
- Workforce security
- Information access management
- Security awareness and training
- Security incident procedures
- Contingency planning
- Evaluation
- Business associate contracts and other arrangements

Physical Safeguards
Business associates and covered entities must have physical safeguards and controls in place to protect PHI. These safeguards focus on the physical access to PHI through facilities, equipment, and other durable resources.

Technical Safeguards
Technical safeguards apply to the systems, operations, and staff required to ensure the protection of PHI.

Access Control:
System activity must be traceable to a specific user. Access controls may include policies, procedures, and processes to support what access needs to be granted, controlled, and monitored.

Equally important is the control of access to update the policies, procedures, and process documentation to ensure that data integrity is maintained. Unauthorized viewing of the data on your computer is a real threat if a computer is ever lost, stolen, or inappropriately decommissioned. A great solution is an encryption.

Access must be restricted via password to authorized employees. Servers and data storage units should be in a secured computer room with limited access. Data should be received and forwarded via automated, electronic processes where no direct human intervention is required. Access or viewing of ePHI should only be allowed when required.

A conversational AI platform should have policies and procedures in place for access control and monitoring to support user identification and tracking. The platform should be set up and configured with active vulnerability monitoring and response systems to protect all data operations.

Audit Controls:
Audit controls must be in place for hardware, software, services, and procedures that record and examine activity in information systems containing or using ePHI.

A conversational AI platform information security management program (ISMP) should have established internal audit procedures to review and monitor the assets, information, data, and user activities associated with ePHI.

Integrity:
The Integrity standard requires a covered entity to implement policies and procedures that will protect PHI from improper alteration or destruction.

Each conversational AI platform deployment includes development, staging, and production configurations that are separated to restrict access and further protect ePHI. Finally, all data on the conversational AI platform is fully encrypted both at rest and in transit using Advanced Encryption Standard (AES)-256, Transport Layer Security (TLS), and Hypertext Transfer Protocol Secure (HTTPS).

Person or Entity Authentication:
A person's identity must be validated to confirm who they are.

A conversational AI application should employ a multi-factor authentication approach to ensure that the person is authenticated on two or more factors, including a one-time authentication with a passcode, token, or a pin code.

Transmission Security:
Covered entities are required to have effective protection of ePHI data-in-motion (data being transmitted electronically). Encryption must be used.

In fact, an excellent conversational AI platform should have a cryptography policy.

Tenets of the policy should include:

- Protection from ePHI being altered
- ePHI shall be rendered unusable if intercepted
- Encryption used for data at rest and data transmission
- Use of symmetric and asymmetric keys where applicable
- Use of non-proprietary, common FIPS-based supported cryptographic algorithms
- No decryption tools stored in the same area as encryption tools

Business Associate's Agreement

The dentist often works with business associates. A business associate is an individual or entity that performs functions or activities that require access to PHI. Associates include entities like suppliers, labs, and other health systems.

HIPAA's Administrative Safeguards require a contract—Business Associates Agreement (BAA)—to be in place with third-party suppliers appropriate to their access, handling,

or use of PHI. Assurances are needed from them to ensure that they understand HIPAA and how to safeguard PHI.

Sometimes a contract is not necessary. Exceptions include but are not limited to:

- Disclosures by a covered entity to a healthcare provider for treatment of an individual
- PHI collection and sharing by a health plan that is a public benefits program, such as Medicare
- Disclosures to a health plan sponsor, by a group health plan, the health insurance issuer, or HMO that provides health insurance benefits or coverage for the group health plan
- With individuals or organizations that are a conduit for PHI, like the US Postal Service

It is necessary to ensure that these third parties only use PHI in a secure and established manner, to help the covered entity carry out its healthcare functions. Business associates must have safeguards in place since they can be held liable to similar repercussions as covered entities.

A conversational AI platform should have an established ISMP that addresses the administrative safeguards required of a business associate. The covered entity would enter into the platform levels of authorization of suppliers and vendors to establish their access to PHI.

The company that develops the conversational AI platform for the covered entity may also need to execute a BAA.

Encryption is Essential

It's important to emphasize that ' password-protected *not* the same as 'secure' or 'encrypted.' As Dentistry IQ puts it, "To understand the difference, think of a padlock and a code. A padlock (like a password) protects against unauthorized access. But once a person unlocks the padlock (gets past the password), the person can see and make sense of everything inside. Encryption, on the other hand, is like a code. The information gets jumbled, so it cannot be used or understood by a person who sees unless that person has the "key" to decode the jumble (the 'encryption key')."

When it comes to a conversational AI platform, all communication between the texting and conversational AI platform and the covered entities' back-end system should be encrypted. Even when on insecure networks, such as at an airport or coffee shop, no one should be able to access PHI. The encrypted platform should use industry-standard AES encryption for stored data, and traffic should be encrypted using TLS 1.2 or greater. Web-based services, including interfaces for all end-user web-based applications, should use HTTPS to protect data transmission.

Storage and servers should also be redundant so that if something fails, the practice can recover quickly. In case of disaster, data must be continuously backed up. Servers should reside in a physically secure data center, monitored 24 hours a day, 365 days a year. The conversational AI platform should continuously identify and update security patches for all of the software used.

A Compliance Checklist

In summary, to comply with the HIPAA Privacy and Security Rules, a conversational AI platform should implement the following:

- Encrypt all stored data with 256-bit AES in Cipher Block Chaining mode
- Encrypt all data as it is transmitted between computers and devices
- No PHI persisted on a phone or a client local system
- Email address verification
- Restrict access to PHI on a need-to-know basis (passwords and company policy)
- Restrict outside access to all servers and production workstations
- Automate data backups
- Store data backups in secured, safe, world-class data centers
- Automate virus checking
- Report any noncompliance
- Allow the U.S. Department of Health and Human Services to audit
- Name a HIPAA Security Official to train staff
- Train all employees with access to PHI on company policies and procedures according to HIPAA mandates
- Relevant training must be required for all new hires and all employees when changes are made to any systems or processes that would affect such controls' performance—or when new risks are introduced.
- Require employees of the conversational AI platform to sign a confidentiality agreement

Best Practices Beyond HIPAA

Hopefully, it is clear now that a texting and conversational AI platform must have a cloud-based HIPAA strategy and built from the ground up with data privacy and security safeguards in place. But there are best practices that go beyond HIPAA. For added security, a texting and conversational AI platform should follow the best practices below for creating even more secure voice assistants.

Anonymized User Accounts:
It's best to use anonymous accounts created and managed within the secure text and voice environment. With this approach, only a unique token is passed from the conversational AI platform to the texting and voice assistant (e.g., Amazon Alexa), and no identifying user account information or PHI is shared with the voice service.

Limit or Disable Voice Cards:
The conversational AI application should allow for posting content to voice "cards" displayed within the voice service account. For example, the Amazon Alexa voice cards' content is visible using Alexa, the Amazon portal, or the Alexa mobile application. It is important to limit the information written to these cards or to use only anonymous accounts.

Limit or Disable Voice Analytics:
Like voice cards, it may be necessary to disable or limit the patient-specific information sent to analytics and reporting services. A conversational AI application should have a feature that narrows the analytics down to a specific voice intent.

Limiting PHI:
Perhaps the most obvious and surest way to deliver patient privacy and data security is to eliminate PHI transmission altogether. Depending on the business need, there are very powerful and valuable voice and text applications that do not require PHI. This may be the best first step into the brave new world of texting and smart voice assistants for many dental healthcare organizations.

Account Linking Using a Secure Provider:
Some skills require the ability to connect an Alexa end user's identity with a user in another system, such as Twitter, Facebook, Amazon, and many others.

For example, suppose you own a web-based service, "*Bye Bye*" that lets users order taxis. It would be very convenient for people to access Bye Bye by voice ("Alexa, ask Bye Bye to order a taxi"). To do that, you'd use a process called account linking, which provides a secure way for Alexa to connect with third-party systems that require authentication.

Account linking leverages OAuth 2.0—an open protocol that provides a simple, standards-based method for web, mobile, and desktop applications to request user authorization from remote servers.

Consider Context:
While texting and voice technology might be secure from how data is protected once it is read or heard by the voice assistant, there are factors to consider outside the technology's control. It is also important to consider the options that make the best sense for the type of information being collected, including the situation or context the person might be in.

For example, only common sense can prevent someone from saying sensitive information to a voice assistant in a crowded room. As a best practice, a form of a warning or notice provided at the start of the conversation or within the dialog can prevent the user from sharing sensitive information.

Application developers and user interface designers should consider the modalities available (voice, chat, touch screens, buttons, etc.) and the data that may be exchanged over these interfaces.

Virtual assistant Cannot Access User Identity

When building a texting and conversational AI platform that will use voice applications like Alexa, there's a lot to think about when you're dealing with PHI. For example, when a patient makes an appointment through your website, they're interacting directly with your site — so protecting that information is relatively straightforward. The health system can wrap that conversation up in HIPAA security.

But with voice applications alone like Alexa, there's a middleman. The user can ask Alexa a question, and that information passes through Amazon on its way to the conversational AI platform. The same goes for Google Assistant and other voice-controlled platforms.

If you're worried about virtual assistants like Alexa accessing user identity, don't be. A conversational AI platform can secure text and voice in a way that ensures Amazon cannot correlate an Amazon account with the user account nor access to PHI secured within the conversational AI platform cloud.

Consider this use case. John Smith is an individual using an Amazon Echo at home to monitor and improve adherence to an experimental prescription drug he's taking as part of a clinical drug trial. The Amazon Echo device allows him to indicate when he's taken medication (e.g., Alexa, I've taken my 9 AM medication) as well as hear a report on his overall medication adherence.

Even though John Smith is using an Amazon Echo to provide information to the conversational AI platform through the voice assistant, Amazon has neither the ability to correlate a relationship between John Smith, Amazon and the conversational AI platform; nor the ability to access any of John Smith's PHI stored securely within the conversational AI platform.

The HIPAA Rules for Emails and Texts

According to Dentistry IQ, the following are rules you can use in your practice to comply with HIPAA, according to Dentistry IQ.

1. **Text messages should not include a patient's PHI. This is true even for texts to staff or other providers inside the same practice. Unless a provider or practice has a secure text messaging platform, text messages are not secure or encrypted. They are easily intercepted, often sent to an incorrect number, and usually stored indefinitely on third-party devices, such as the wireless carrier's servers.**

2. **Dentists who want to text or email patients must use a messaging system that encrypts messages or requires patient login, or obtain the patient's consent for using unencrypted email or text messages to communicate with the patient after advising the patient of the risks of doing so, including the risk that the message could be read by a third-party.**
3. **The above rules do not apply to emails or texts sent by a patient. Patients can use unencrypted emails and texts. However, if the provider believes the patient might not understand the risks of sending unencrypted email or texts or if the provider has concerns about potential liability, the provider may want to alert the patient of those risks.**
4. **Including a confidentiality notice or disclaimer in an email or text does not make it compliant with HIPAA.**

Conclusion

A texting and conversational AI platform for a dental practice need to be HIPAA-compliant to referring dentists, labs, and patients securely. The ideal platform will remove barriers to become the go-to tool for collaboration and clinical case management. Imagine integrated text and voice-assisted, guided data entry for ordering implants, supplies, and equipment, as well as integrated capabilities for intelligent conversational experiences with voice assistants such as Alexa and Google Assistant.

Amazon announced in 2019 that a version of their virtual assistant technology, Alexa, is HIPAA-eligible. This means that it's available for applications that are subject to the data privacy and security requirements of HIPAA and that Amazon is willing to consider executing a BAA with Alexa skill developers who want to create HIPAA-compliant skills. As of this writing (March 2020), the new HIPAA-eligible version of Alexa is available to a limited number of developers by invitation only from Amazon.

This opens up opportunities. A dentist on a conversational AI platform could theoretically have the ability to access health information via a skill for Alexa and provide more personalized and timely insights through voice – the most natural and convenient user interface in the home.

There is clear value in a text and conversational AI platform for dental practice and the dental industry, but it will be used at significant risk if it is not within a secure system. The HIPAA Privacy Rule and Security Rule are the bare requirements. It is recommended that given the sensitive nature of health data and changing policies with new technologies like voice AI, going beyond these HIPAA rules will serve you best.

About Awrel

The Awrel Connect™, by Awrel LLC, is dentistry's first HIPAA-compliant texting application using a hands-free voice assistant built on a conversational AI platform. Dentists and others can use the Awrel application to improve workflow by leveraging a virtual assistant that acts as a workflow template to do any number of tasks through the power of voice, conversational interfaces, and secure text.

Companies using Awrel Connect™ and Awrel Voice™ can private-label their offerings, define unique workflows, and create company and product-specific offerings.

Awrel was established to ensure that the dental industry utilizes technologies that bring affordable tools to the industry for regulatory compliance, practice growth, profitability, improved patient outcomes, and a heightened level of practice and business satisfaction.

References:

Christi Olson. "New Report Tackles Tough Questions On Voice and AI," Blog, https://about.ads.microsoft.com/en-us/blog/post/april-2019/new-report-tackles-tough-questions-on-voice-and-ai, 4/23/19.

Dentistry IQ. "Emails, texts, and HIPAA: 7 rules every dentist needs to know", https://www.dentistryiq.com/practice-management/patient-relationships/article/16366021/emails-texts-and-hipaa-7-rules-every-dentist-needs-to-know, 6/29/17.

U.S. Department of Health and Human Services. "Summary of the HIPAA Privacy Rule," Health Insurance Portability and Accountability Act, https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

U.S. Department of Health and Human Services. "Summary of the HIPAA Security Rule," Health Insurance Portability and Accountability Act, https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html, 1996.

SSL2Buy. "Symmetric vs. Asymmetric Encryption – What are differences?", https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences.

U.S. Department of Health and Human Services. "Business Associates," Health Insurance Portability and Accountability Act, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html, 1996.

Amazon Alexa. "Understand Account Linking for Alexa Skills," https://developer.amazon.com/en-US/docs/alexa/account-linking/understand-account-linking.html.

OAuth 2.0. "What is OAuth and Why Does It Matter?", https://oauth.net/.

Arnold Rosen. Awrel App, https://app.awrel.com/login.

Arnold Rosen. Awrel, Awrel.com.