Codify
BY AAPC

Health Information Compliance Alert

Technology Trends: Think Twice Before Jumping on Board the Virtual Assistant Bandwagon

Remember: No BAA, no deal.

Information technology has propelled medicine into areas never thought possible, aiding clinicians with the delivery of enhanced, efficient care. And though most practices could use an extra pair of hands to assist with notetaking or research, some tech trends skirt the fine line of compliance.

Case in point: Personal virtual assistant technology like Apple's Siri, Amazon's Alexa, and Google Assistant - among others - are now ubiquitous in homes. The technology is so available that many people even wear it, via smart watches or through their phones, which are always on hand.

While you may rely on the ease and convenience of these handsfree notetaking and scheduling services in your private life, you should tread very carefully if you're considering using them at the office.

Reflect on the Consequences of Using Such a Device in Your Practice

The companies that make these devices are honest about the lack of security. Amazon, for example, has business associate agreements (BAAs) available for the **Amazon Web Services** (AWS) branch of the company, which offers cloud storage for electronic protected health information (ePHI). AWS keeps a continually updated list of services that are compatible with the HIPAA Privacy Rule.

"There is no HIPAA certification for a cloud service provider (CSP) such as AWS. In order to meet the HIPAA requirements applicable to our operating model, AWS aligns our HIPAA risk management program with FedRAMP and NIST 800-53, which are higher security standards that map to the HIPAA Security Rule. NIST supports this alignment and has issued SP 800-66 An Introductory Resource Guide for Implementing the HIPAA Security Rule, which documents how NIST 800-53 aligns to the HIPAA Security Rule," says the AWS website.

But even if your practice already has a BAA in place with AWS, the agreement doesn't cover the Amazon Alexa or Echo devices.

"Customers may use any AWS service in an account designated as a HIPAA account, but they should only process, store, and transmit protected health information (PHI) in the HIPAA-eligible services defined in the business associate addendum (BAA)," the AWS website says.

Look to what each company explicitly mentions when figuring out HIPAA compliance. If you're hoping that an Amazon Alexa or Echo will have a place in your practice, you may be in luck at some point in the future.

"AWS follows a standards-based risk management program to ensure that the HIPAA-eligible services specifically support the security, control, and administrative processes required under HIPAA. Using these services to store and process PHI allows our customers and AWS to address the HIPAA requirements applicable to our utility-based operating model. AWS prioritizes and adds new eligible services based on customer demand," the AWS website says.

Google's Home speaker offers similar convenience for personal use with the same caveats in a medical practice.

Know How the Devices Work - and Collect Data

While the devices aren't constantly recording conversations, they're still "listening."

Both devices are listening for the words to activate their services. Google calls these words or phrases "hotwords" and you can train or retrain your device to respond to your preference.

"Google Home listens in short (a few seconds) snippets for the hotword. Those snippets are deleted if the hotword is not detected, and none of that information leaves your device until the hotword is heard," Google says.

Understand These Major Security Concerns

If you're still considering having one of these devices somewhere in your office, even just to play music more easily, reevaluate the larger security concerns. Oftentimes, the convenience that these devices offer means they inherently compromise your privacy and data.

"To help you [work] faster and more easily, a service might use information from past conversations with you, even if they happened on different Google Home devices ... All services are required to register a privacy policy that explains what information they record and how they use it. The privacy policy must also explain how you can control the way they use your information. To read a service's privacy policy, look it up under the services page in the Google Home app," Google says.

But those privacy policies don't include HIPAA compliance. And these devices are not physically secure or secured within your network.

Besides physically walking off with one of these devices, a savvy questioner can elicit information from the Google Home device easily.

"Anyone who is near your Google Home device can request information from it, and if you have given Google Home access to your calendars, Gmail or other personal information, people can ask your Google Home device about that information. Google Home also gets information about you from your other interactions with Google services," Google says.

Food for thought: Apple currently does not have any information on Siri's HIPAA compliance, but experts and laymen agree that it does not meet compliance standards.

Bottom line: "I wouldn't recommend the use of any of these devices in a medical office, primarily due to HIPAA," says **Harlene S. Stevens, CPA**, manager at **Nisivoccia LLP** in in Arlington, New Jersey.

Resources: Stay updated with device compliance straight from the companies through these links at https://aws.amazon.com/compliance/hipaa-eligible-services-reference/ and >https://support.google.com/googlehome/answer/7072285?hl=en&vid=0-914378488769-1529669571487.