Codify
BY AAPC

MDS Alert

HIPAA: Alexa May Be Helpful, But Don't Roll Out the Welcome Mat Just Yet

A device that can answer questions, remember things, and engage lonely residents sounds like a godsend - but in terms of compliance, virtual assistant devices in nursing facilities may be too good to be true.

Technology-based virtual assistants like Google Home, Amazon Alexa or Amazon Echo, or Apple Siri may have carved out a niche in modern life, but should their presence (and people's dependence upon them) really extend into healthcare settings - especially residential situations?

While some long-term care facilities are testing pilot programs to see whether facilities can successfully integrate these personal virtual assistants into resident and staff life, there are very real privacy and compliance risks associated with jumping on the virtual assistant bandwagon.

They're Always Listening

Residents may feel isolated if they receive less attention or have fewer chances to engage in conversation than they did at their previous home or residence. A device that listens and responds - no matter how many times a question is asked - can feel like a godsend for anyone involved or familiar with such a situation.

But listening - one of the virtual assistants' greatest strengths - also makes the devices extremely dangerous in a healthcare setting.

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

"The way that it works is that it sits there and the device is monitoring for its commands. So it listens for 'Alexa' and the command that you're giving it. And when the device hears that command - those words that it knows - it captures a certain amount of information and it records it, all along. It sends the last few seconds before it heard [the command] and the few seconds after that," says **Donna Grindle**, founder and CEO of **Kardon Compliance**, on the podcast Help Me With HIPAA (of which she is also a co-founder and co-host).

All of these snippets are then sent away from the device to the Amazon Cloud, where they're processed by Amazon's powerful speech recognition resources. The information is then distilled and sent back to the device, where it is provided in the form of an answer, Grindle says.

The Google device works in a similar way, with the slight lingo difference of the commands or phrases being called "hotwords." Google points out that 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.

The devices are designed to listen, which is problematic, but the way they must store information - which lets them regurgitate information for you or provide a local weather forecast, for example - is what really compromises their safety, in terms of privacy.

Both Amazon and Google are open about these privacy issues.

"To help you 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. The potential issues only compound if the devices belong to residents.

Devices Don't Play Well With HIPAA

Amazon provides clear directives to Echo users that its virtual assistant services are not compliant with the Health Information Portability and Accountability Act(HIPAA).

Amazon, for example, has business associate addendums (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 Health Information Portability and Accountability Act (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 facility already has a BAA in place with AWS, the agreement doesn't cover the Amazon Echo devices or Alexa services.

"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.

Devices' Vulnerability an Attribute of Design

These devices are designed to be portable, present, and ready to respond at the drop of a hat. But their size and portability marks them as especially vulnerable to different kinds of cyberattack - or even old-fashioned put-it-in-your-pocket-and-walk-away theft.

Besides physically walking off with one of these devices, a savvy questioner can elicit information from the Google Home device easily. And with elderly people already targeted for fraud and theft, allowing devices that can access and store a wealth of personal information means taking on extra risk.

"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.

"Voice assistants have different levels and types of security for stored information. In speaking with an attorney out of New Jersey, there was something that came up about how the iPhone's Siri keeps recordings and transcripts but ties them to random numbers, making the users more anonymous. Amazon's Alexa is less secure, for example. It stores full transcripts that can be viewed by anyone who can access the account. So you've created data - be aware of where that data is stored and who can access that data," says **Terry Fletcher, BS, CPC, CCC, CEMC, CCS, CCS-P, CMC, CMCSC, CMCS, ACS-CA, SCP-CA**, owner of **Terry Fletcher Consulting Inc.** and consultant, auditor, educator, author, and podcaster at CodeCast, in Laguna Niguel, California.

Compliance May Be in Devices' Future

If these customer service-oriented companies continue to hear about how their devices could be more useful - and,

therefore, how they can get their services into more people's lives - they are apt to make the necessary investments to figure out a way that their devices could become compliant.

"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.

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

Bottomline: Though personal virtual assistant devices may offer a boon to individual residents, think very carefully before allowing the technology into your facility. The risks of breaches and other unsafe privacy issues probably outweigh the benefits of convenience to residents and staff.

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