BLUE ORANGE®
COMPLIANCE

Smart Speakers and Voice-Controlled Devices in Senior Care: New Opportunities and Risks

New technologies and the Internet of Things (IoT) ignite possibilities – and privacy challenges for senior living

The current generation of senior citizens was born into what was considered at the time to be a new world of electronic devices such as the camera, telephone, radio, and phonograph. Technology advances over their lifetime introduced these device lovers to television, tape recorders, video, personal computers, electronic games, smartphones, and the internet. Throughout this evolution, each new tool often incorporated desirable elements from a previous device but also required new skill sets, forcing society – including residential care environments – to adapt and adopt policies to accommodate these enhanced tools.

The amazing ability to integrate all these technologies and devices, as well as new ones that will continue to be developed, is being called the Internet of Things, or IoT, which creates a distinct combination of opportunities and risks. The IoT has not only brought many promising technologies to older adults who have limited mobility or access to certain services, but equally allows them to continue enjoying what technology has provided throughout their lives.

For senior living providers, IoT devices such as smart speaker/voice-controlled digital assistants[1] (or ambient listening devices) can be a boon for enhancing the lives of their residents. Although the focus here is on Voice-controlled Devices (VcD) – and the current state of this technology because it is changing at an accelerated pace – there is a myriad of other detection and communication devices that are also part of the IoT.

The evolving opportunities are endless with current IoT “listening” and sometimes “seeing” devices particularly useful in reducing loneliness; reminding users about appointments, nutrition or medication; and bringing the world to people without having to use a computer keyboard. These devices and the things they are interacting with are getting more versatile at a tremendous pace.

In senior living alone, residents can use a VcD to communicate with the nursing station or housekeeping, they can find out when their care is scheduled, or when activities are available. They can also learn from other IoT devices like “Fitbit-type” wearable monitors and have that information communicated to care-givers or even family members. The VcD can provide companionship directly or by serving as a portal to loved ones, it can entertain and can certainly enhance resident experiences and satisfaction. Equally important, a care provider can communicate information and reminders via the VcD to a specific resident, improving quality, efficiency, and outcomes.

As with any new technology used in a semi-private setting, reasonable-use parameters are necessary, as is the ability to provide technical support. From an information-security standpoint, it is prudent to not connect IoT devices (including VcDs) to the network that is used for its corporate, financial, health or other sensitive information until reasonable and current technical protections are in place. With billions of devices forecast to be on the market soon – and each with variable security ratings – they will become ubiquitous in society,

[1] Amazon Echo Dot (Alexa), Apple HomePod, Apple Siri, Google Home and Assistant, and Microsoft Cortana, among others.

including among older adults. Like smartphones today, they are likely to become part of every environment so having solid policies and procedures in place is imperative.

In April 2019, Amazon announced that its Alexa Skills Kit now enables select covered entities and their business associates to handle health information as part of an invitation-only program. As VcDs continue to advance in the healthcare space, this is good news for the industry.

Amazon has developed a HIPAA-compliant method for a defined set of Amazon "healthcare skills" for those six covered entities. This will allow people who are clients of the six organizations to interact using Alexa and their defined relevant health data will be stored and maintained by that organization.

Amazon's announcement that its Alexa Skills Kit enabling select covered entities and their business associates to handle health information as part of an invitation-only program is good news as VcDs continue to advance in the healthcare space.

However, the Amazon announcement does not mean that Alexa can be used unilaterally as HIPAA compliant. Senior living organizations covered by HIPAA should continue to follow recommended guidance for non-HIPAA compliant VcDs. Please note that there are vendors that have created HIPAA compliant management software allowing them to be implemented in senior living settings as well as other healthcare settings.

Develop a thoughtful security and privacy plan for all IoT devices in long-term and post-acute (LTPAC) care

Although the opportunities are great for senior living providers and those they serve, there are also risks when allowing or using a VcD or similar IoT devices. To begin with, the location where these devices will be used is a factor. There are many questions to consider:

- Will they be deployed in a nursing unit, assisted living, or independent living community – or perhaps a life plan community with all of those settings?
- Will they only be in private rooms or apartments, or in shared rooms, nurse stations, treatment areas, or common spaces?
- Will a community choose to provide such devices as an amenity or simply accommodate residents who bring their own?
- Will the VcD be owned by the facility, or sold/leased to the resident?
- Will the device be enabled with acceptable security and accompanied by facility-acceptable use guidance and procedures?

According to the *National Law Review*[2], as healthcare providers continue to design new ways to use VcDs, the challenge remains that these devices are not in themselves "compliant with federal privacy law protections under the Health Insurance Portability and Accountability Act (HIPAA). Although HIPAA compliance is expected to occur in the near future, the proper technical and security safeguards have not been implemented."

Even though there are minimum privacy and information-security standards in the HIPAA regulations that were developed many years ago, they did not anticipate IoT. More recent state laws may be more restrictive, and the journal warns any use of a VcD or other IoT devices "would also have to be compliant with applicable state law."

The *National Law Review* also calls attention to the passive "listening" capability with regard to HIPAA and Electronically Protected Health Information (ePHI). Many IoT devices are designed to identify acoustic patterns that match the "wake word" that has been created. "This capability creates the foreseeable possibility that information, including protected health information, will be recorded, whether intended to or not. Accordingly, the security measures in place for storing such information becomes of critical importance to defend against hackers."

If protected data is recorded, simply storing that information in a cloud system (which is required for most of these devices to function) without the appropriate protections/agreements may be a breach on its own. In most cases the VcD technology allows the microphone to be turned off, theoretically preventing audio from streaming to the cloud, even when the user says the chosen wake word. Also, with most VcDs the voice recordings associated with a user's account can be reviewed and deleted, either one-by-one or all-at-once. While good to know, managing these factors for multiple residents has the potential to become extremely complicated with potential compliance and other legal implications.

The *National Law Review* recommends that providers undergo a privacy and information-security review to ensure all state and federal legal and regulatory requirements are met prior to the implementation of new technology.

The *National Law Review* suggests safeguards that healthcare providers can implement:

1. **Until Alexa becomes HIPAA compliant, any use of the device should be limited to non-identifiable health information;**
2. **Once Alexa is HIPAA compliant, providers will need to execute a Business Associate Agreement with Amazon or its related entities;**
3. **Providers should implement and revise their policies and procedures to ensure device use is compliant with HIPAA; and**
4. **Providers should update their privacy notice to include the use of Alexa or other voice-enabled devices.**

Using Alexa and other Voice-Controlled Devices (VcDs) in senior living and care settings

Depending on how the VcD is used – and in which settings – providers have much to consider. Following are examples of some possible situations and what roles providers, caregivers, and clinicians might play in each setting.

Nursing Homes (NHs)

The NH[3] environment, as a defined covered entity, must always comply with HIPAA/HITECH regulations and adopt evolving procedures to conform with new technologies. Among other things, these procedures need to address

[2] "Alexa…What is HIPAA?" written by Kristen Andrews Wilson from © Steptoe & Johnson PLLC. All Rights Reserved.

potential business associates and workforce training, anticipating and protecting against ePHI breaches, all within a framework of resident rights. In a NH setting, there are a number of benefits for a resident who uses a device for assistance and entertainment. There are situations with minimal privacy or information-security concerns such as when a resident listens to music, accesses information on the internet, or simply operates the television. These are, of course, relatively harmless activities.

But for administrators there are also risks that lurk beneath the surface with regard to privacy, information-security, and regulatory compliance. It is useful for an administrator to have a privacy and information-security consultant provide current suggested conforming procedures. ePHI is indeed a primary concern. Remember, these devices are always "on" and "listening," possibly observing and documenting. While the VcD is an excellent tool in many ways as it fields verbal requests directly, it may also record communication between caregivers and residents that may include talk considered to be ePHI.

Voice-enabled technology is developing rapidly and can be highly beneficial for clinicians in multiple ways, especially in a NH setting. Soon, a clinician, nurse or certified nursing assistant (CNA) may use a voice-controlled virtual assistant to obtain a resident's electronic health record, remind a resident to exercise, or prompt voiding. It may be used during a physician visit to accurately capture examinations and therefore support accurate coding and billing. The administrator must, of course, be aware that any type of interactive recording will probably be accessible for Quality Assurance purposes, as well as third-party audits. So, when VcD tools are allowed or provided by the facility, that facility should be skilled at maintaining and securing these tools and including them as part of the annually required risk assessment.

In addition, VcDs can also be used for entertainment, for example playing the resident's favorite music, or keeping them socially connected and engaged with family and potentially peers and staff.

Assisted Living Settings

The VcD has broad appeal throughout the senior living sector. Communities may provide devices as an amenity to families or the residents themselves and enhance the concierge services provided. Perhaps even more common currently is the interest among seniors to bring their own personal devices with them at move-in.

While concern for the user's own privacy and information security is more obvious, it is also important to consider the privacy of neighbors who may visit the user's apartment and inadvertently share health information conversationally. A VcD has the capacity to record this information, most likely unbeknownst to the visitor. Information shared and/or recorded between residents is probably not considered legally protected information, but the facility needs to consider the ramifications and their potential liability if prudent precautions are not in place. This is where privacy and information-security consultants can provide many suggested best practices.

Another potential liability for assisted living providers is when home-health caregivers provide services in the resident's apartment. Because resident rooms are typically modest in size, the resident and caregiver are likely to exchange health information within earshot of a VcD without remembering that it is passively "listening"

[3] Includes CMS-regulated SNF, ICF, Transitional Care, Sub/Post-Acute, Rehabilitation, and ICF-MR facilities.

for the wake-up phrase. Depending on how the assisted living provider needs to comply with state or federal privacy requirements, they along with the home-health provider should be aware of how the VcD is intentionally or passively involved with health information privacy, cybersecurity, and documentation issues. The risks in this situation could rise to HIPAA violations if the ePHI is breached due to an unsecured network or other unmitigated risks.

Independent Living

If an independent living community chooses to offer a VcD to each of its new residents as an amenity, there are particular issues that come with that decision. While information security and privacy may not be regulated for independent living communities, the liability and community's reputation is still a concern for the ownership. Similar to the assisted living scenario, a resident might engage a home healthcare agency. When the VcD or network is owned by the community and sensitive information may be stored, the healthcare provider might need to have a business relationship agreement with the community or authorization from the resident indicating the recognition of the device and its functions. As in other residential community settings, the community must take responsibility for how listening devices will be secured against potential violations.

Even in the case of residents bringing their own VcDs to a community, the provider may face state privacy laws because, although the community is not a regulated healthcare setting, the law may apply to any environment. In addition, the provider's WIFI networks should maintain reasonable protections and mitigate vulnerability to outside attacks.

Life Plan Communities

Since life plan communities encompass many or all of the aforementioned settings, operators need to take precautions at the highest and perhaps more stringent level for the enterprise. NF, assisted living, and independent living on one campus and under the auspices of one corporate entity warrant a more comprehensive approach to internet and data security, possibly using firewalls and other tools to either segregate or integrate data in ways that are the most effective for the organization. Being aware of a desire to serve residents who move among care settings within the community means taking a reasoned approach that can make information compliance easier to manage across departments and settings.

Additional Considerations

Whose device is it? While a community must be well-prepared regardless of who owns a VcD, there is a level of risk. In the situation where residents bring their own devices, providing a secured, protected, and perhaps dedicated WIFI network is advisable. Secure a signed agreement with the resident (and possibly device manufacturer) that covers expected management of malware and ePHI. While the compliance bar may be higher, it is actually easier to control security measures and procedures by providing and managing the devices for each interested resident. This ensures that all devices and networks are configured consistently and to the community's identified best practices – particularly as these policies and procedures change over time, as technology and related challenges evolve.

Caregiver use. Although not yet commonplace, direct caregivers, nurses, and physicians are beginning to use VcDs and other IoT devices to monitor care, retrieve medical records and other data, or document care. In

these cases, senior living providers should be thoughtful about how those devices connect to the community's network. The risk of HIPAA violations center around how well the connection is secured and the ePHI is protected. The provider's responsibility is significant when ePHI or financial data is involved.

Internet access. Whether the technology is supplied or simply accommodated, careful thought should be given to how that device will access the internet. If the resident gets internet access through a guest or IoT network, the community is taking on responsibility of providing a reliable and secure connection to the devices. If instead devices are connected to an internet connection owned by the resident, the community may only be expected to provide basic guidance and assistance. Regardless which type of setup is selected, both have inherent security concerns and it is imperative to use best practices to secure the connection.

Fog computing. Voice-enabled devices frequently rely on fog computing, a decentralized computing infrastructure in which all the processing happens on devices physically closer to where the data is collected, instead of sending data to the cloud. While allowing for faster processing, fog computing adds another layer of complexity to personal assistant technologies.

Subnet. A reasonable interim modification that communities might consider is putting in place a subnet and rules that will isolate IoT use from other data generated by the community. The life plan community can then require all listening devices to use the subnet for a more focused point of control. Having residents sign indemnification agreements or authorizations is also a good idea.

Policies, procedures, education. To ensure compliance, it would be wise for any healthcare or senior living provider to modify and enforce all policies, procedures, and training programs to mitigate the accepted risks associated with the deployment and use of VcDs that are appropriate to the care setting, application, and usage circumstances. Related to this, and important to remember, is to perform an annual information-security risk assessment, and document effective workforce training around the regulatory protections and the providers' own policies and procedures. Having not only the technical experts, but every team member onboard – and compliant – is essential and no small task.

Technical expertise. To enhance capabilities and reduce liability, every new technology comes with its own unique need for technical expertise. For all of these care and living environments, it will be prudent to have workforce members or vendors that know how to not only keep the VcD functioning, but also protect the individuals and the provider from unnecessary concern while understanding and managing the organizational privacy, security, and compliance risk introduced by the use of these devices. Focusing on uses that don't involve sensitive information is always a good place to begin. Some providers will want to experiment with apps and tools provided by the VcD manufacturer and others will wait for bugs to be worked out before trying them. There are even VcD platform tools currently available specifically for healthcare.

Legal considerations. Because VcDs may mishear a word that sounds like the wake word, they open up a new concern as possible digital evidence in law suits. While companies may be resistant to releasing information stored in the cloud, a subpoena can demand this evidence of resident-care encounters. As a precaution, providers should consult with their legal counsel regarding the inclusion or amending of resident contracts to account for privacy and/or liability issues related to VcDs.

Develop a thoughtful plan for all IoT devices in long-term and post-acute (LTPAC) care

The major components of a solid information-security and privacy strategy for voice-enabled technology in the LTPAC setting should include:

- Keeping devices and resident data secure from unauthorized parties.
- Securing enterprise data to ensure that it is not accessed by or via voice-enabled devices.
- Conforming to pertinent privacy and security laws, such as HIPAA, state, and other regulations.
- Limiting legal exposure by ensuring that resident information is not compromised by any form of negligence or by the inadvertent recording of situations involving resident care that could be used inappropriately or in a way that could be damaging.

The intersection of IoT, internet security, healthcare, and senior living certainly creates exciting opportunities, but also a complex set of challenges that warrant careful monitoring and vigilant compliance. Pay attention to related topics from industry associations, literature, trade media, and knowledgeable vendors that analyze these issues. Providers are advised to consult legal, privacy, and information-security experts to keep up with best practices.

To learn how BlueOrange Compliance helps communities protect themselves and their residents, call 855.500.6272 or visit www.blueorangecompliance.com.

About BlueOrange Compliance:

BlueOrange Compliance specializes in assisting healthcare organizations navigate HIPAA and HITECH Privacy and Security requirements. Complex, ever-changing healthcare regulations and increasing risks make it difficult for organizations to stay in front of emerging cyberthreats. As a single source, we equip every client with affordable, practical, comprehensive privacy and security solutions, including multiple sources of information to help manage risk. Our clients have peace of mind knowing they are compliant and prepared for potential breaches and adverse audits.